Kleshchev **Algebra**
Student Solution Manual

Chapter 1 through 5

James Wilson

Published: December 3, 2003

Department of Mathematics
1222 University of Oregon
Eugene, OR 97403-1222

jwilson7@darkwing.uoregon.edu
www.uoregon.edu/ jwilson7/

Written with LaTeX 2_ε.

Please Recycle when finished.

This is the product of a graduate level algebra course taken at the University of Oregon, 2002-2003, under the instruction of Alexander Kleshchev. The solutions are mostly the work of the author, James Wilson, while the exercises were developed by Kleshchev. Many exercises appear in common texts, such as Hungerford's Algebra and Rotman's Advanced Modern Algebra.

I developed the solutions as a preparation for the Ph.D. qualifying exams. With the exception of some parts of chapter 2, most of the solutions have been proof read to some degree. However, mistakes are bound to exist still. My hope is that these may help others with many of the common problems encountered when preparing for qualifying exams. Having passed the exams, my advice in using these notes is to **do each problem yourself.**

I welcome any comments and corrections you may have. I would also like to thank Professor Kleshchev, David Hill, Alex Jordan, and Dragos Neacsu for their advice on certain solutions.

Contents

Chapter 1

Groups

---

1 Cyclic Groups – True or False? Let G be a group such that any finitely generated subgroup of G is cyclic. Then G is cyclic.

Hint: Consider the Prüfer group $Z(p^\infty)$.

Example: Of course the assertion is too good to be true, and we find a counter example in the Prüfer group $Z(p^\infty)$. The geometric description of the Prüfer group is the rotations of all p^n-gons, for all $n \in \mathbb{N}$. These are all inscribed one in the next. The subgroups, thus, form a chain of cyclic groups, and so any finite number of generators is generated by a generator with highest order, that is, that all finitely generated subgroups are cyclic. However, the entire group is not cyclic as certainly it is not isomorphic to $\mathbb{Z}$ which has the subgroups $2\mathbb{Z}$ and $3\mathbb{Z}$ which are not in a chain. $\square$

2 Transitive Embedding Let G be a finite group with $|G| > n$. Then G is isomorphic to a transitive subgroup of S_n if and only if G contains a subgroup H of index n such that neither H nor any proper subgroup of H is normal in G.

Hint: Consider G acting on G/H.

Proof: Suppose H is a subgroup of index n in G which is not normal and which has no proper normal subgroups. Let us take G to act on the left cosets G/H. This induces a homomorphism $G \to S_n$ whose kernel must be contained in H (as $gH \neq H$ whenever $g \notin H$.) However, H is not normal, nor are any of its proper subgroups, so the only option we have is to choose the kernel as $\langle 1 \rangle$. This kernel shows we have a monomorphism so G is represented faithfully in S_n. Since the action of G on G/H is always transitive, the representation of G in S_n is transitive.

Now that the mystery is explained we consider the reverse implication. Begin with G a transitive faithful embedding of G in S_n. Then we must have an monomorphism $G \to S_n$. This induces a natural action of G on n elements. This action is G-isomorphic to G acting on G/G_1 by [Kle03, Theorem-1.5.5]. The action is transitive so the size of the orbit is n which forces the size of index of the stabilizer G_1 in G to be n.

All that remains is to show no non-trivial subgroup of G_1 is normal in G – including G_1. Suppose there where a normal subgroup N in G contained in G_1. Since G_1 is conjugate to G_i for all $i = 2, \dots, n$, then in fact N – which is invariant under conjugation – is in each G_i. However we know the intersection of all G_i's is trivial – since it is precisely the kernel of the faithful embedding of G – and it would certainly contain N; thus, N must be trivial. $\square$

3 Probability of Commutativity Let G be a finite group. We choose an element $g \in G$ randomly, then replace it and make another random choice of an element $h \in G$. Prove that the probability that g and h commute equals $k/|G|$, where k is the number of conjugacy classes in G.

Hint: Use Brunside's Formula[Rot02, Thm-2.113] and centralizers.

Proof: Given a fixed $g \in G$, the probability of choosing an element $h \in G$ which commutes with g is the same as the probability of selecting something from the centralizer, so $|C_G(g)|/|G|$. Since this is for a specific element we must average over all the elements. As the group action is conjugation, $C_G(g) = Fix(g)$ so we get:

$$P = \frac{1}{|G|} \sum_{g \in G} \frac{|C_G(g)|}{|G|} = \frac{1}{|G|} \left(\frac{1}{|G|} \sum_{g \in G} |Fix(g)| \right) = \frac{k}{|G|}.$$

Notice the second step applies the Burnside's Lemma [Rot02, Thm-2.113]. $\square$

Hint: Show either a subgroup is a copy of $\mathbb{Z}$, or there are infinitely many cyclic subgroups of finite order.

4 Infinite Groups Any infinite group has infinitely many subgroups.

Proof: When a group G is infinite it has an infinite number of elements; thus it must certainly contain a countable subset which we enumerate $\{a_i \mid i \in \mathbb{N}\} \subseteq G$, where $a_i = a_j$ if and only if $i = j$.

Each element generates a subgroup $A_i = \langle a_i \rangle$ of G. For each subgroup A_i we have two options: it is infinite, or it is finite. If any such subgroup is infinite then it is isomorphic to $\mathbb{Z}$ which has the infinite list of subgroups $m\mathbb{Z}$ for each $m \in \mathbb{Z}$; therefore, A_i has an infinite number of subgroups and so so must G.

Not having been forced into this option, consider the alternative that every A_i is finite. Once again consider the subgroups $\langle a_i \rangle$. There is no reason to suspect that each $\langle a_i \rangle$ is distinct; several generators for each could appear in one group. However, these subgroups are a subset of the lattice of subgroups of G and therefore they are partially ordered. If there is an infinite chain, or an infinite number of finite chains, then there are infinitely many subgroups.[1] Therefore suppose that there are only a finite number of chains and that each is finite length.

This requires that an infinite number of elements be packaged in a finite number of subgroups all of which are finite. A finite number of finite sets has only a finite number of elements; therefore, this last case cannot be. So G must have an infinite number of subgroups. $\square$

Hint: Leverage the (proper) maximality of subgroups to show two way set containment.

5 Frattini Subgroup Let G be a finite group. The *Frattini subgroup* $\Phi(G)$ is the intersection of all maximal subgroups of G. An element $g \in G$ is called a *non-generator* if whenever $\langle X, g \rangle = G$, we have $\langle X \rangle = G$ for subsets $X \subseteq G$. Show that $\Phi(G)$ is the set of non-generators of G.

Proof: Suppose an non-generator g is not in the Frattini subgroup. Take any maximal subgroup M which does not contain g (which exists since $g \notin \Phi(G)$). Since M is maximal, it follows:

$$\langle M, g \rangle = M \vee \langle g \rangle = G.$$

Since it is assumed to be a non-generator then $\langle M \rangle = G$. Of course this violates the assumption of M, since M is a maximal proper subgroup. Thus g is in the Frattini subgroup.

Given any element $g \in \Phi(G)$, if $\langle X, g \rangle = G$ suppose $\langle X \rangle \neq G$. Whatever $\langle X \rangle$ is, it is contained in a maximal subgroup M then. But this means $\langle X, g \rangle = \langle X \rangle \vee \langle g \rangle$ can be no more than M since g and X are both in M. Thus $\langle X, g \rangle \neq G$. So this last contradiction proves our assertion: the Frattini subgroup is the group of all non-generators. $\square$

Hint: $Aut(\mathbb{Z}_n) = \mathbb{Z}_n^\times$.

6 Cyclic Automorphisms – True or False? $Aut(C_8) \cong C_4$.

Example: The assertion is false. We know $Aut(C_8) = \mathbb{Z}_8^\times$ where $\mathbb{Z}_8^\times = \{[m] \in \mathbb{Z}_8 \mid (m, 8) = 1\}$ under multiplication. Certainly the order of the group is 4, but it is the Klein 4 group not C_4. We see this because

$$\begin{aligned} 3^2 = 9 &\equiv 1 \pmod 8 \\ 5^2 = 25 &\equiv 1 \pmod 8 \\ 7^2 = 49 &\equiv 1 \pmod 8. \end{aligned}$$

Thus all the non-trivial elements are of order 2, so no element is of order 4 so the group cannot be C_4. $\square$

[1] The first case can be seen in the Prüfer group.

7 Maximal p-subgroups Let G be a finite group and p be a prime. Show that there exists a normal p-subgroup $O_p(G)$ such that $H \leq O_p(G)$ for any normal p-subgroup H in G. Show that there exists a normal subgroup $O_{p'}(G)$ of order prime to p such that $H \leq O_{p'}(G)$ for any normal subgroup H in G whose order is prime to p.

Hint: Recall if N is normal, then $N \vee H = NH$. Also, the join of normal subgroups is normal, as is the intersection.

Proof: Consider $\{H_i \mid i \in I\}$ as the collection of all p-subgroups of G which are normal in G. Since G is finite it can only have a finite number of subgroups so we can denumerate our H_i's as $H_1, \dots, H_n$. Since they are normal their join is simply their complex, that is, that

$$O_p(G) = \langle H_1, \dots, H_n \rangle = H_1 \cdots H_n.$$

We observe this set will be $O_p(G)$ since it, by construction, contains all normal p-subgroups. Since the normal subgroups of a group form a complete modular lattice, we in fact know the join of these normal subgroups is normal.[2] Moreover, we use the complex to give us the necessary counting arguments to determine its order as $|H_1| \cdots |H_n|$. Since these are all subgroups of a finite group their orders are respectively finite and so this product is finite; in fact, they are all p-subgroups so our resulting group is non-other than a p-subgroup with all the properties of $O_p(G)$.

Now suppose we take $K_1, \dots, K_m$ to be all normal subgroups with orders relatively prime to p. Then again using the normal lattice properties we see

$$O_{p'}(G) = \langle K_1, \dots, K_m \rangle = K_1 \cdots K_m,$$

and once again this is normal; it contains all the K_i's; and it it has order $|K_1| \cdots |K_m|$. Since p does not divide any $|K_i|$ it follows it will not divide their product; thus, $O_{p'}(G)$ has all the properties we require. $\square$

8 Minimal p-quotients Let G be a finite group and p be a prime. Show that there exists a normal subgroup $O^p(G)$ such that $G/O^p(G)$ is a p-group, and $H \geq O^p(G)$, for any normal subgroup H in G such that G/H is a p-group. Show that there exists a normal subgroup $O^{p'}(G)$ such that $[G : O^{p'}(G)]$ is prime to p, and $H \leq O^{p'}(G)$, for any normal subgroup H in G with $[G : H]$ prime to p.

Hint: Recall if N is normal, then $N \vee H = NH$. Also, the join of normal subgroups is normal, as is the intersection.

Proof: Let $\{H_i : i \in I\}$ be the family of all normal subgroups of G whose quotient groups are p-groups. As the normal subgroups form a complete lattices, we may consider the normal subgroup

$$H = \bigcap_{i \in I} H_i.$$

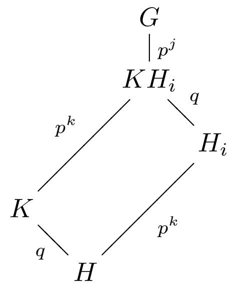
Clearly $H \leq H_i$ for all $i \in I$. Now we wish to show $[G : H] = p^n$ for a suitable n.

Suppose a prime $q \neq p$ divides $[G : H]$. Then there is an element a of order q in G by Cauchy's Theorem[Kle03, Thm-1.5.25]. Thus by the correspondence theorem [Kle03, Thm-1.4.15], we may pull back a subgroup K which corresponds to $\langle a \rangle$ under the projection of G onto G/H. Hence the complex KH_i for any $i \in I$, is a subgroup above both H and H_i. However, $[KH_i : H_i] = q$ which

[2] We see this also by a direct check:

$$gH_1 \cdots H_n g^{-1} = gH_1 g^{-1} gH_2 g^{-1} \cdots gH_n g^{-1} = H_1 \cdots H_n.$$

shows that G/H_i is not a p-group. Thus no q other than p divides $[G : H]$ so H is the group $O^p(G)$.



The existence of $O^{p'}(G)$ is the identical argument, only we assume p does divide $[G : H]$ and show the impossibility. $\square$

Hint: Use the characterization of nilpotent groups as products of Sylow subgroups together with the fact that the join of normal subgroups is the complex.

9 Nilpotent Subgroups – True or False? If G is a finite nilpotent group, and m is a positive integer dividing $|G|$; then there exists a subgroup of G of order m.

Proof: True, indeed even a normal subgroup of order m can be found. Given every finite nilpotent group is a product of its Sylow subgroups, we may write

$$G \cong P_1 \times \cdots \times P_n,$$

where $|P_i| = p_i^{k_i}$ is the Sylow p_i-subgroup for each i. Moreover, for every P_i there is a chain of normal subgroups in P_i

$$\mathbf{0} = P_i^0 \lhd P_i^1 \lhd \cdots \lhd P_i^{k_i} = P_i$$

with $|P_i^j| = p_i^j$.[3] Finally we note that if $N \lhd H$ then $N \times \mathbf{0} \lhd H \times K$; thus, each P_i^j is normal in G in a canonical way.[4]

Now we have the tools to construct our desired groups. Take $m|n$, and express m in primes:

$$m = p_1^{m_1} \cdots p_n^{m_n}.$$

As the complex with a normal subgroup is a subgroup we see we may take

$$H = P_1^{m_1} P_2^{m_2} \cdots P_m^{m_n}$$

to be a subgroup of G, and furthermore we can know the order is simply m. What is more, as each $P_{i,j}$ is normal in G we are in the normal subgroup lattice so we have indeed constructed a normal subgroup of order m in G. $\square$

Hint: Consider any element in $G \backslash H$.

10 Classification of "Local" Groups A non-trivial group G has a proper subgroup H which contains every proper subgroup of G. What can you say about G? (Another version: Let G be a finite group such that for all subgroups $H, K \leq G$, we have $H \leq K$ or $K \leq H$. What can you say about G?)

Example: Indeed the classification is that $G \cong C_{p^i}$ for some prime p and some $i \geq 1$. Since $G \neq H$, $G \backslash H$ is non-empty, so take an element $a \in G \backslash H$. Notice

[3] We know the center of a p-group is non-trivial, and every subgroup of the center is normal, so we may find a normal subgroup of order p. Then we quotient the p group by this subgroup, repeat the process to find a new normal subgroup of order p, use the correspondence theorem to pull it back to the original and thus construct a chain of p-powered normal subgroups.

[4]
$$(a,b)N \times \mathbf{0}(a^{-1}, b^{-1}) = aNa^{-1} \times \mathbf{0} = N \times \mathbf{0}.$$

$\langle a \rangle \leq G$ so either $G = \langle a \rangle$ or $\langle a \rangle \leq H$ by the hypothesis on H. Yet a avoid H so we are forced to conclude that G is cyclic and generated by a.

Now to complete the classification we assume G is infinite and immediately know $G \cong \mathbb{Z}$ so there are distinct maximal subgroups $2\mathbb{Z}$ and $3\mathbb{Z}$ which prove G does not fit the hypothesis. Thus G must be finite. But if $p, q|n$, where $n = |G|$ then the subgroups $\langle a^{n/p} \rangle$ and $\langle a^{n/q} \rangle$ have index p and q respectively; thus, once again we have distinct maximal subgroups. Therefore only one prime divides the order of G and G is cyclic so $G \cong C_{p^i}$.

Indeed the lattice for G is a chain as suggested by the alternate version. □

11 p-subgroup Chains Let G be a finite group. For each prime p dividing $|G|$, let $S_p(G)$ denote the set of all p-subgroups of G. Suppose for each p dividing $|G|$, that $S_p(G)$ is totally ordered by inclusion (i.e.: we have $H \leq K$ or $K \leq H$ for any $H, K \in S_p(G)$). Prove that G is cyclic.

Hint: Show G is a product of its Sylow subgroups then invoke Exercise-1.10 to conclude each Sylow subgroup is cyclic.

Proof: Since $S_p(G)$ is totally ordered and G is finite, there is a top element in each chain, and so we take $P_1, \ldots, P_n$ to be the respective top elements of the chains of each p_i dividing the order of G. Notice conjugation is an automorphism so it must send subgroups to subgroups of the same order, but there is a unique subgroup of maximal p_i-th order for each i so we see that each P_i is indeed normal in G. Moreover, as there orders are relatively prime these groups can only intersect trivially – precisely stated [5]

$$P_i \cap P_1 \cdots \hat{P}_i \cdots P_n = \mathbf{0}.$$

Furthermore from the pigeon-hole principle we know

$$G = P_1 \cdots P_n$$

so the stage is set to conclude that

$$G = P_1 \times \cdots \times P_n.$$

Now we recall one final step: in Exercise-1.10 we saw a finite group whose lattice is a chain is simply a cyclic group, so now we may say:

$$G \cong C_{p_1^{i_1}} \times \cdots \times C_{p_n^{i_n}}$$

so G is cyclic by the classification of cyclic groups. □

12 Counting Involutions – True or False? If G is a group with even number of elements, then the number of elements in G of order 2 is odd.

Hint: Partition G into pairs $\{a, a^{-1}\}$ then count.

Proof: The assertion is true. The result falls from the abstraction of a common notion for groups. Suppose we define an action of $C_2 = \{1, -1\}$ on a group G by $g \cdot x = x^g$ where $g \in C_2$ and $x \in G$. There are only two issues to check: $1 \cdot x = x^1 = x$, and

$$g(hx) = g(x^h) = x^{hg} = x^{gh} = (gh)x.$$

This natural action makes orbits out of an element and its inverse; thus, each orbit has one or two elements; furthermore, orbits of size one correspond precisely to the trivial element or elements of order 2.

The orbits induced on G are a partition of G so their sizes must sum to G. When $|G| = 2n$, the elements of the orbits must add up to $2n$. If we let k be

[5] The hat means skip this entry.

the number of orbits of size two, then we must remove $2k$ from $2n$ to indicate the number of elements remaining; so there are $2(n-k)$ elements in orbits of size one. However, we know the trivial element will always be in an orbit of size one because it is its own inverse. This leave an odd number, $2(n-k)-1$, of non-trivial elements, all of which are in orbits of size one and so by construction are elements of order two. $\square$

Hint: S_3.

13 Nilpotent Extensions Show if N is a normal subgroup of G, and both N and G/N are nilpotent, G still may not be nilpotent.

Example: Consider the group S_3. The subgroup $\langle(1\ 2\ 3)\rangle$ is normal in S_3 because it has index 2. Since it is also cyclic it is nilpotent. Thus S_3/A_3 is nilpotent and A_3 is nilpotent. However, S_3 is not since the center of S_3 is trivial, proving the lower (ascending) central series never begins.[6] $\square$

Hint: Consider D_8.

14 Normal Transitivity – True or False? If X is a normal subgroup of Y and Y is a normal subgroup of Z, then X is a normal subgroup of Z.

Example: The transitivity of normality is generically false. The first place we can test this meaningfully is with the groups of order 8. Naturally we will look into non-abelian groups where normality is questionable – specifically D_8 since we know Q_8 is Hamiltonian.

For convince, represent D_8 in S_4 as the group $\langle(1\ 2\ 3\ 4),(1\ 3)\rangle$. Notice the subgroup $F=\langle(1\ 3)\rangle$ is of index 2 in the subgroup $K_4=\langle(1\ 3),(2\ 4)\rangle$ so F is normal in K_4; likewise, K_4 is of index 2 in D_8 so it is normal in D_8. We have our setup.

The subgroup F is easy to conjugate because it has only one non-trivial subgroup. Take $(1\ 2\ 3\ 4)$ in D_8 and conjugate F:

$$(1\ 2\ 3\ 4)F(1\ 4\ 3\ 2)=\{(1),(2\ 4)\}\neq F.$$

Since F is not invariant under conjugation in D_8 it is not normal in D_8 and so we see normality may not be transitive. $\square$

Hint: Use the second isomorphism theorem.

15 Examples of the Parallelogram Law Let G be a finite group and $N\trianglelefteq G$. If $(|N|,[G:N])=1$, prove that N is the unique subgroup of G having order $|N|$.

Proof: Suppose N_1 and N_2 are normal subgroups of G satisfying the hypothesis and where $|N_1|=|N_2|$. Then their complex is their join. Notice

$$[N_1:N_1\cap N_2]|N_1\cap N_2|=|N_1|=|N_2|=[N_2:N_1\cap N_2]|N_1\cap N_2|$$

so $j=[N_1:N_1\cap N_2]=[N_2:N_1\cap N_2]$ and by the parallelogram law (second isomorphism theorem would also work), $j=[N_1N_2:N_1]=[N_1N_2:N_2]$. We see this in the following diagram.

$$\begin{tikzcd}
 & G \arrow[d, dash, "i"] & \\
 & N_1N_2 \arrow[dl, dash, "j"'] \arrow[dr, dash, "j"] & \\
N_1 \arrow[dr, dash, "j"] & & N_2 \arrow[dl, dash, "j"'] \\
 & N_1\cap N_2 \arrow[d, dash, "k"] & \\
 & \mathbf{0} &
\end{tikzcd}$$

[6]Notice this is a special case of a family of such examples: the dihedral groups of orders not a power of 2.

$[G:N_1]=[G:N_1N_2][N_1N_2:N_1]=ij$ and since

$$|N_1|=[N_1:N_1\cap N_2]|N_1\cap N_2|=jk$$

we see that we require $(jk,ij)=1$ to satisfy our assumptions on N_1; therefore, $j=1$, so $N_1=N_2$ as $[N_1:N_1\cap N_2]=1$. $\square$

16 The Complex Subgroup Let G be a finite group and $H,K\leq G$ be subgroups. Then HK is a subgroup of G if and only if $HK=KH$.

Hint: Recall any proof of NH being a subgroup when N is normal. The normal form $HK=KH$ replaces the need for normality.

Proof: Let H,K be subgroups of G and presume the complex HK is a subgroup of G. Since HK contains K ($1\in H$, so $1\cdot k\in HK$ for all $k\in K$) it will be closed to conjugation by K. Given any $h\in H$, $k\in K$, $hk\in HK$ by construction, and therefore $k(hk)k^{-1}=kh\in HK$. So $KH\subseteq HK$, and by the symmetric argument, $HK\subseteq KH$ so in fact $HK=KH$.

Now suppose $HK=KH$. Given $1\in H$ and $1\in K$, $1\cdot 1=1\in HK$ proving HK is non-empty. Take $h,h'\in H$ and $k,k'\in K$, so that we choose arbitrary elements $hk',h'k\in HK$. Since $KH=KH$ there is some $h''\in H$, $k''\in K$ such that $k'h'=h''k''$. With this, the product $hk'h'k$ becomes $(hh'')(k''k')$ which is visibly in HK; therefore, HK is closed to products. Also, $(hk)^{-1}=k^{-1}h^{-1}\in KH$ so in fact $(hk)^{-1}\in HK$. Therefore HK is a subgroup of G. $\square$

17 Parallelogram Law If H,K are subgroups of G, then $[H:H\cap K]\leq[G:K]$. If $[G:K]$ is finite, then $[H:H\cap K]=[G:K]$ if and only if $G=HK$.

Hint: Consider the bijection $hH\cap K\to hK$.

Remark 1.0.1 *If we allow for a certain abuse of notation we may even say* $[H:H\cap K]=[HK:K]$*, where* $[HK:K]$ *denotes the cosets of* K *over* HK *even if* HK *is not a subgroup. This reveals the truly combinatorial nature of the proof.*

Proof: Let $H/H\cap K$ and HK/K denote the sets $\{hH\cap K\mid h\in H\}$ and $\{gK\mid g\in HK\}$ without any assertions of group structure on $H/H\cap K$, HK or HK/K. With this define a map $\varphi:H/H\cap K\to HK/K$ as $hH\cap K\mapsto hK$. The map is well-defined if whenever $hH\cap K=h'H\cap K$ it follows $hK=h'K$. But this is equivalent to asking that $h^{-1}h'H\cap K$ map to K. Since $h^{-1}h'H\cap K=H\cap K$ it follows $h^{-1}h'\in H\cap K$ so indeed $h^{-1}h'\in K$; thus, $h^{-1}h'K=K$ so φ is well-defined.

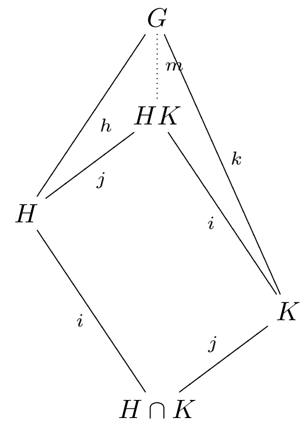
Given $h\in H$ such that $hK=K$ it follows $h\in K$ and so $h\in H\cap K$ so $Ker\ \varphi\leq H\cap K$. For any $h\in H\cap K$, clearly $h\in K$ so $hK=K$ and thus $Ker\ \varphi=H\cap K$. Thus φ is injective. For all $g\in HK$, $g=hk$ for some $h\in H$ and $k\in K$. Thus $gK=hkK=hK=\varphi(hH\cap K)$ so φ is surjective and even now bijective. So we conclude $[H:H\cap K]=[HK:K]$ where the abused notation is understood.

As a corollary we see $HK\subseteq G$ so $[H:H\cap K]\leq[G:K]$. Whenever G is finite, the pigeon-hole-principle proves $[H:H\cap K]=[G:K]$ if and only if $G=HK$. $\square$

18 HK-subgroup If H and K are subgroups of finite index of a group G such that $[G:H]$ and $[G:K]$ are relatively prime, then $G=HK$.

Hint: Notice $[G:K][K:H\cap K]=[G:H][H:H\cap K]$.

Proof: We let $[G:K]=k$, $[G:H]=h$, $[H:H\cap K]=i$, and $[K:H\cap K]=j$. Then we have the following subset lattice (notice the labels on the lines indicate the index of the lesser in the greater):



$H \cap K$ is a subgroup in G. Furthermore both $[G : H]$ and $[G : K]$ are finite indices, so by the Lemma of Poincaré ([Hun74, Proposition-I.4.9]) we know $[G : H \cap K] \leq [G : H][G : K]$ and is therefore finite. From the Theorem of Lagrange ([Hun74, Theorem-I.4.5]) we know: $[G : H][H : H \cap K] = [G : H \cap K] = [G : K][K : H \cap K]$, which are all finite products.

We must resolve when $hi = kj$ knowing $(h, k) = 1$. Since h and k are relatively prime it follows $h|j$ and $k|i$, so $h \leq j$ and $k \leq i$. But by Proposition-I.4.8 we see $j = [K : H \cap K] \leq [G : H] = h$ and likewise $i \leq k$. Therefore $i = k$ and $j = h$. Finally Proposition-I.4.8 concludes since $[H : H \cap K] = [G : K]$ then $G = HK$. $\square$

Hint: The maximal subgroups have index 2 and intersections of normal subgroups are normal.

19 Hamiltonian Groups – True or False? All subgroups of Q_8 are normal.

Example: This is true as Q_8 is a Hamiltonian group. To see this notice the elements i, j, k all determine distinct subgroups of order 4 – which means they have index 2, so they are normal. These maximal subgroups intersect at $\langle -1 \rangle$ and since the normal subgroups form a lattice, this intersection is normal. The only subgroups remaining are the entire group and the trivial group both of which are trivially normal. Thus all subgroups are normal.

That these are indeed all the subgroups follows from the observation that the only element of order 2 is -1, so there can be no $C_2 \times C_2$ subgroups, and all the cyclic order 4 subgroups are accounted for. $\square$

Hint: Conjugate using cycles and the fact that conjugation permutes indices.

20 Center of S_n The center of S_n is trivial for $n \geq 3$.

Example: Let $n > 2$ and consider the center of S_n. Since disjoint cycles are independent of each other we may test for centrality on just the elements in the cycle. Given a central element σ, pick a cycle $\kappa = (a_1, \dots, a_i)$, with $2 < i \leq n$ out of σ which consequently must also be central.

Next take τ to be $\tau = (a_1, a_2)$. Now conjugate:

$$\kappa\tau\kappa^{-1} = (a_1, \dots, a_i)(a_1 a_2)(a_i, \dots, a_1) = (a_2 a_3) \neq \tau.$$

Therefore κ is not central forcing σ to be the same.

This leaves us only the case where σ is a product of disjoint transpositions. Now consider a cycle in such an element: it must take the from $\kappa = (a_1, a_3)$. But since $n > 2$ we know there exists a $\tau = (a_1, a_2, a_3)$ and we simply conjugate:

$$\kappa\tau\kappa^{-1} = (a_1, a_3, a_2) = \tau^{-1} \neq \tau.$$

So once again neither κ nor σ are central, so indeed the center of S_n is trivial. $\square$

21 Parallelogram Example If $N \trianglelefteq G$, $|N|$ is finite, $H \leq G$, $[G : H]$ is finite, and $[G : H]$ and $|N|$ are relatively prime, then $N \leq H$.

Hint: Draw a parallelogram then justify the index of the desired side is 1.

Proof: We know $[G : H]$ is finite so $[NH : H]$ is finite and as always it follows $[NH : H] = [H : N \cap H]$. Also $|N|$ is finite so from the theorem of Lagrange we know

$$|N| = [N : H \cap N]|H \cap N| = [NH : H]|H \cap N|$$

(where all the pieces here are finite) and $[G : H] = [G : NH][NH : H]$; thus, since these two numbers are relatively prime, it follows $[NH : H] = 1$ so $N \leq H$. $\square$

22 $\mathbb{Q}$ subgroups $(\mathbb{Q}, +)$ does not have subgroups of finite index.

Hint: Use the index of the subgroup to annihilate any element in the quotient group.

Proof: Given any subgroup H of $\mathbb{Q}$ we know H is normal in $\mathbb{Q}$ as $\mathbb{Q}$ is abelian. Let $n = [\mathbb{Q} : H]$. By the theorem of Lagrange every element in $\mathbb{Q}/H$ as order dividing n. So carelessly take any coset $\frac{a}{b} + H$ and write

$$\frac{a}{b} + H = \frac{na}{nb} + H = n\left(\frac{a}{nb} + H\right) = 0.$$

Thus $\mathbb{Q}/H$ is trivial so $n = 1$ and thus all proper subgroups of $\mathbb{Q}$ have infinite index. $\square$

23 Finite Index Intersections If H and K are finite index subgroups in G, then so is $H \cap K$.

Hint: Use the Parallelogram Law (Exercise-1.17).

Proof: Recall from the Parallelogram Law that $[H : H \cap K] \leq [G : K]$. Yet $[G : K]$ is finite so $[H : H \cap K]$ must also be finite. Now we use the Lagrange's Theorem to see

$$[G : H \cap K] = [G : H][H : H \cap K]$$

which is a product of finite numbers so it is finite. $\square$

24 Unions of Conjugation If H is a proper subgroup of finite a finite group G, then the union $\bigcup_{g \in G} gHg^{-1}$ is not the whole G. [See also Exercise-1.25.]

Hint: Make an estimation of the order of the union from the index of the normalizer.

Proof: The number of subgroups conjugate to H is given by the index of the normalizer $N_G(H)$ in G. As $H \neq G$ it follows if H is normal it conjugacy class contains only itself so G is not the union of the conjugate subgroups of H. So we therefore know H is strictly contained in $N_G(H)$ so indeed $1 < [G : N_G(H)] < [G : H]$. Now let n denote the cardinality of $\bigcup_{g \in G} gHg^{-1}$. As the identity is in common with each gHg^{-1}, and possibly more, we may bound n as follows:

$$n \leq [G : N_G(H)](|H| - 1) + 1 \leq [G : H](|H| - 1) + 1 = [G : H]|H| - [G : H] + 1.$$

Using the theorem of Lagrange we see this is simply:

$$n \leq |G| - [G : H] + 1 < |G|,$$

the last step justified as $[G : H] > 1$. Thus the cardinalities do not agree so that G is not the proposed union. $\square$

Hint: Mimic Exercise-1.24 using $G/\bigcap_{g\in G} gHg^{-1}$ as a set (not as a group) instead.

25 Unions of Conjugation If $H < G$ and of finite index, then G is not the union $\bigcup_{g\in G} gHg^{-1}$.

Proof: The number of subgroups conjugate to H is given by the index of the normalizer $N_G(H)$ in G. As $H \neq G$ it follows if H is normal it conjugacy class contains only itself so G is not the union of the conjugate subgroups of H. So we therefore know H is strictly contained in $N_G(H)$ so indeed $1 < [G : N_G(H)] < [G : H] < \infty$.

We also pause to provide a technical result: $[G : H] = [G : gHg^{-1}]$ for any group G and subgroup H and element $g \in G$. To see this take a transversal T of G/H – as a set only (that is a subset of G for which $h, k \in T$, $hH = kH$ implies $h = k$ and $G/H = \{kH \ : \ k \in T\}$). This is because

$$\bigcup_{k\in T} kH = G = gGg^{-1} = \bigcup_{k\in T} gkHg^{-1} = \bigcup_{k\in T} gkg^{-1}gHg^{-1} = G/gHg^{-1}.$$

So we see the natural bijection of transversal so the indices are equal. Thus both are also finite as one is.

Now take $K = \bigcap_{g\in G} gHg^{-1}$. As there are only finitely many subgroups conjugate to H, by induction and Exercise-1.23 we have that the intersection of finitely many subgroups of finite index is of finite index as well.

Treating H/K as the set $\{hK \ : \ h \in H\}$ we let n denote the cardinality of $\bigcup_{g\in G} g(H/K)g^{-1}$. As the identity is in common with each $g(H/K)g^{-1}$, and possibly more, we may bound n as follows:

$$\begin{aligned} n &\leq [G : N_G(H)]([H : K] - 1) + 1 \leq [G : H]([H : K] - 1) + 1 \\ &= [G : H][H : K] - [G : H] + 1 = [G : K] - [G : H] + 1 < [G : K], \end{aligned}$$

the last step justified as $[G : H] > 1$. Hence the conjugate subgroups do not cover the elements in the quotient (as a set only) so they will not cover the elements in the inter group G. $\square$

Hint: Use Exercise-1.25 to show that the subgroup generated by these elements cannot be proper.

26 Conjugacy Classes and Generators Let G be a finite group G, and $g_1, \ldots, g_l$ be representatives of the conjugacy classes of G; then $G = \langle g_1, \ldots, g_l\rangle$.

Proof: Let $H = \langle g_1, \ldots, g_l\rangle$. We must show H is not a proper subgroup of G. Since we have a representative from each conjugacy class it follows $G = \bigcup_{g\in G} gHg^{-1}$. However form Exercise-1.25 we know this cannot occur (note since all is finite certainly $[G : H]$ is finite) so H must be G itself. $\square$

Hint:

27 $GL_n(\mathbb{F}_q)$ The group $GL_n(\mathbb{F}_q)$ has an element of order $q^n - 1$.

Proof: Consider $\mathbb{F}_{q^n}$ as a $\mathbb{F}_q$ vector space. It is clear that the dimension is n so as an abelian group it splits as

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q^n.$$

Now $GL_n(\mathbb{F}_q)$ is precisely the group of all linear automorphisms of $\mathbb{F}_q^n$; therefore, also of $\mathbb{F}_{q^n}$ in a natural way. However we know that set of linear automorphisms of $\mathbb{F}_{q^n}$ contains $\mathbb{F}_{q^n}^\times$ and furthermore that any finite subgroup of the multiplication of a field is cyclic – so indeed

$$\mathbb{F}_{q^n}^\times \cong C_{q^n-1}.$$

Thus $GL_n(\mathbb{F}_q)$ contains a copy of C_{q^n-1}. So indeed there is an element of order

$q^n - 1$ in $GL_n(\mathbb{F}_q)$. [7] $\square$

28 Conjugate Cluster Let H be a subgroup of a group G. Let

$$C := \{g \in G \mid H \cap gHg^{-1} \text{ has finite index in both } H \text{ and } gHg^{-1}\}.$$

Show that C is a subgroup of G.

Hint: For closure show $H \cap ghHh^{-1}g^{-1}$ contains $H \cap gHg^{-1} \cap hHh^{-1}$.

Proof: Notice of course $H \cap 1H1 = H$ so $1 \in C$ proving C is non-empty.

Next take $g, h \in C$. From Exercise-1.23 we know

$$[H : H \cap gHg^{-1} \cap hHh^{-1}]$$

is finite as $[H : H \cap gHg^{-1}]$ and $[H : hHh^{-1}]$ are both finite. Now we need only show that $H \cap ghHh^{-1}g^{-1}$ contains $H \cap gHg^{-1} \cap hHh^{-1}$ and we will have shown that $[H : H \cap ghHh^{-1}g^{-1}]$ is finite since then

$$[H : H \cap ghHh^{-1}g^{-1}] \leq [H : H \cap gHg^{-1} \cap hHh^{-1}].$$

Moreover, mutatis mutandis, we will have $[ghHh^{-1}g^{-1} : H \cap ghHh^{-1}g^{-1}]$ finite as well so we will be able to conclude that $gh \in C$.

Well certainly if $u \in H \cap gHg^{-1} \cap hHh^{-1}$ then $huh^{-1} \in H$ which means $ghuh^{-1}g^{-1} \in H$ so indeed any u in this given intersection also lies in $ghHh^{-1}g^{-1}$. So we have our desired set containment.

Finally take $g \in C$. We know $[H : H \cap gHg^{-1}]$ is finite as is $[gHg^{-1} : H \cap gHg^{-1}]$. Now simply conjugate by g^{-1}. Since conjugation is an automorphism the indices must be preserved; thus,

$$[gHg^{-1} : H \cap gHg^{-1}] = [g^{-1}gHg^{-1}g : g^{-1}(H \cap gHg^{-1})g] = [H : g^{-1}Hg \cap H]$$

is finite and

$$[H : H \cap gHg^{-1}] = [g^{-1}Hg : g^{-1}(H \cap gHg^{-1})g] = [g^{-1}Hg : g^{-1}Hg \cap H]$$

is as well, so $g^{-1} \in C$. $\square$

29 3 Sylow-2-subgroups Suppose that a finite group G has exactly three Sylow 2-subgroups. Show that every permutation of these Sylow subgroups can be obtained by conjugation by some suitable element in G.

Hint: Act on the Sylow subgroups by conjugation and show that the kernel of the action cannot contain all three Sylow-2-subgroups.

Proof: Let G act on the Sylow-2-subgroups by conjugation. It follows this action is closed as Sylow-2-subgroups can only be conjugate to other Sylow-2-subgroups in a finite group. Moreover the action is transitive so the induced homomorphism $f : G \to S_3$ must cover A_3. That is to say that $[G : Ker\ f] \geq 3$. So we have only two choices: $[G : Ker\ f] = 3$ or $[G : Ker\ f] = 6$ in which case f is surjective. If f is surjective then we have confirmed that every permutation of the Sylow-2-subgroups can be had by appropriate conjugating elements.

Now suppose instead that $[G : Ker\ f] = 3$. As G as distinct Sylow-2-subgroups it must therefore have non-trivial Sylow-2-subgroups so indeed 2 divides the order of G. Moreover now we see that as $[G : Ker\ f] = 3$, every

[7] The element in question can be determined as

$$A = \begin{bmatrix} 1 & & \cdots & & 1 \\ & & & 1 & 0 \\ \vdots & & \iddots & \iddots & \vdots \\ & 1 & & & \\ 1 & 0 & \cdots & & 0 \end{bmatrix}$$

Sylow-2-subgroup must be contained inside $Ker\ f$ or otherwise the index would be even by the correspondence theorem. However we may also characterize the kernel as the intersection of all the normalizers. If we take S_1, S_2 and S_3 to be the Sylow-2-subgroups, then $S_1, S_2, S_3 \leq Ker\ f \leq N_G(S_1)$ so it follows that S_1 is not conjugate to S_2 or S_3 inside $N_G(S_1)$. However, S_1 is a Sylow-2-subgroup of $N_G(S_1)$ so it must be conjugate to all other Sylow-2-subgroups in $N_G(S_1)$ which contradicts the previous result. Therefore $Ker\ f$ cannot contain all the Sylow-2-subgroups so indeed $[G : Ker\ f] = 6$. □

Hint: Consider that left regular action on a finite index subgroup.

30 Infinite Simple Groups Prove that any infinite simple group G has no subgroup of finite index.

Proof: Suppose G is an infinite simple group with a subgroup H of finite index n. Certainly G acts transitively on the left cosets of H so there is an induced homomorphism $f : G \to S_n$. Since G is simple, the kernel of f may only be trivial or G. A trivial kernel requires the impossibility of embedding an infinite number of elements in a finite group. Making G the kernel forces the action of the left cosets to be trivial, not transitive. With no options left, we conclude H was a fantasy to begin with. □

Hint: Consider Sylow-5-subgroups and show G is then impossibly embedded in A_6.

31 Simple Groups of order 120 Prove that there is no simple group of order 120.

Proof: From the third Sylow theorem it follows there are either 1 or 6 Sylow-5-subgroups. If G is to be simple then there must be 6. Thus conjugation induces a homomorphism $f : G \to S_6$. Moreover, the kernel must be trivial if G is simple, thus f is and embedding. If G is not completely contained in A_6 then $G \cap A_6$ is a normal subgroup of G. Thus $G \leq A_6$. However this cannot be as $[A_6 : G] = 6!/(2 \cdot 120) = 3$ and we know to keep A_6 simple there can be no subgroup of index $2, \ldots, 5$.

So while it is possible to have a 6 Sylow-5-subgroups – for example S_5 – it is not possible to avoid a normal subgroup somewhere in G. □

Hint: Count the Sylow subgroups.

32 Simple Groups of order $2^4 7^2$ The groups of order $2^4 \cdot 7^2$ are not simple.

Example: The number of Sylow 7-subgroups r_7 must divide $2^4 \cdot 7^2$ and be congruent to 1 modulo 7. The possible choices are 1,2,4,8, and 16. Of these only 1 is congruent to 1 mod 7. Therefore there is one Sylow 7-subgroup.

Since conjugation is an automorphism, a lone Sylow 7-subgroup must be invariant to conjugation and thus it must be normal. Therefore all groups of this order are non-simple. □

Hint: Notice $5^2 \nmid (6-1)!$

33 Simple Groups of order 150 Prove that there is no simple group of order 150.

Proof: Using [Kle03, Thm-1.7.13] we know a group of order $150 = 2 \cdot 3 \cdot 5^2$ is not simple as $(5, 6) = 1$ yet $5^2 \nmid 5!$. □

Hint: Consider conjugation on Sylow-2-subgroups.

34 Simple Groups of order 80. Show that a group of order 80 must have a non-trivial normal subgroup of order a power of 2.

Example: By the third Sylow theorem we knew a group G of order 80 has either 1 or 5 Sylow-2-subgroups. If it is 1, then G has a proper normal subgroup of order a power of 2, as requested. So presume that now there are 5 Sylow-2-subgroups.

As Sylow-2-subgroups are conjugate we have an induced homomorphism $f : G \to S_5$ which represents the action of conjugation on the Sylow-2-subgroups. As 80 does not divide 120, we are forced to acknowledge there is a non-trivial kernel for f. Moreover, if g any element in G, then if $gHg^{-1} = H$ for every Sylow-2-subgroup H, then $g \in N_G(H)$ for each H. However, the index of every Sylow-2-subgroup in G is prime, 5, so $N_G(H) = H$ or else H would be normal in G. Hence we see that the kernel of f lies inside the Sylow-2-subgroups of G and so there is a non-trivial proper normal 2-subgroup of G. □

35 **D_8 Representation** Prove that the group of upperunitriangular 3×3 matrices over $\mathbb{F}_2$ is isomorphic to D_8.

Hint: Use v. Dyck's theorem.

Proof: Let $U_3(\mathbb{F}_2)$ be upperunitriangular matrices and define the map $f : D_8 \to U_3(\mathbb{F}_2)$ on the generators as follows:

$$f(a) = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}; \qquad f(b) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It is easy to verify $f(b)^2 = I_3$ and

$$f(a)^2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \qquad f(a)^4 = I_3.$$

Now

$$f(b)f(a)f(b)^{-1} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = f(a)^{-1}.$$

Now that we have satisfied all the relations we use v. Dyck's Theorem to conclude f extends to a homomorphism from D_8 to $U_3(\mathbb{F}_2)$. Moreover, the kernel of f is trivial as the order of $f(a)$ and a and $f(b)$ and b agree. Finally, $|U_3(\mathbb{F}_2)| = 2^3 = 8$ so by the pigeon-hole principle f is surjective so f is an isomorphism. □

36 **Trivial Relations** Let G be a finite group with $g \sim g^2$ for every $g \in G$. Prove that $G = \mathbf{1}$.

Hint:

Remark 1.0.2 *The following proof is an exercise in killing a flee with an atomic bomb; it should not be viewed as the best proof.*

Proof: Let $a \in G$ and take $g \in G$ so that $a^2 = gag^{-1}$. Since conjugation is an isomorphism, it follows the order of a^2 is that of a. Thus the order of a is odd. Moreover since every element has odd order, the order of the group must be odd so it must be solvable.

Now notice

$$[g, a] = gag^{-1}a^{-1} = a^2a^{-1} = a$$

so $G = G'$. Since G is solvable, but has as a derived series that does not start, it follows G is the trivial group. □

37 **2 Conjugacy Classes** Suppose that a finite group G has exactly two conjugacy classes. Determine G up to isomorphism.

Hint: The order of each conjugacy class must divide the order of the group.

Proof: One conjugacy class must always be that of the trivial element, and it contains exactly this one element. By our assumption all other elements of G are in the second conjugacy class. If G has order n then we are saying there is a conjugacy class of order $n-1$. However since this is an orbit, it must divide the order of G so in fact $n-1|n$. Since $(n-1,n)=1$ the only case this can occur is when $n=2$. Thus $G \cong C_2$. $\square$

Hint: Let S_4 act on its Sylow-2-subgroups.

38 S_4 – True or False? $S_4/V_4 \cong S_3$.

Proof: This is true. We know the number of Sylow-2-subgroups is 1 or 3 by the third Sylow theorem. Easily we see there are 6 elements of the form (a,b), and three of the from $(a,b)(c,d)$. All these having order 2 must be contained in some Sylow-2-subgroup, but there are 9 and the order of the Sylow-2-subgroups is 8, so there must be 3 Sylow-2-subgroups, not 1.

From Exercise-1.29 we know that S_4's action on the Sylow-2-subgroups by conjugation yields a surjection onto S_3. Thus we have $f: S_4 \to S_3$ and all we need to identify is the kernel so we may conclude that $S_4/V_4 \cong S_3$ by the first isomorphism theorem.

In particular, the subgroups of order 4 are cyclic or $C_2 \times C_2$. In the first case $\langle(1234)\rangle$ is conjugate to $\langle(1324)\rangle$ via (23) so they cannot be normal. Likewise $\langle(12),(34)\rangle$ and $\langle(13),(24)\rangle$ are conjugate via (23) again. So the only order 4 subgroup that is normal in S_4 is V_4. Thus it must be the kernel. $\square$

Hint: Every element of order 5 is of the form $(a_1,\ldots,a_5)$.

39 Transitive Subgroups of S_5 – True or False? Every subgroup of order 5 of S_5 is transitive.

Proof: This is true. A subgroup of order 5 must be a cyclic subgroups and thus corresponds entirely to elements of order 5 in S_5. When we write an element as a product of disjoint cycles $\alpha = \alpha_1 \cdots \alpha_n$ we immediately know its order to be the least common multiple of the length of each cycle α_i. Since 5 is prime it follows the only permutations that can be of order 5 are those which are a product of disjoint length 5 cycles. However we only have 5 elements to act on so each element of order 5 in S_5 takes the form $\alpha = (a_1,\ldots,a_5)$ with $\{a_1,\ldots,a_5\} = \{1,\ldots,5\}$. Without loss of generality let $a_1 = 1$ – we can rotate the permutation until this is so – and choose any point $b = 1,\ldots,5$. It follows $b = a_i$ for some $i = 1,\ldots,5$ so indeed $\alpha^i(1) = b$ so the orbit of 1 is $\{1,\ldots,5\}$ so the group $\langle\alpha\rangle$ acts transitively. As this is an arbitrary order 5 subgroup of S_5 we know all subgroups of order 5 in S_5 are transitive. $\square$

Hint: Any (the) non-abelian group of order pq will serve.

40 pq-groups – True or False? If p and q are primes, then a group of order pq is nilpotent.

Example: As with Exercise-13, the group S_3 serves as an example. The order of S_3 is pq where $p=2, q=3$ but it is not nilpotent because its center is trivial; thus its upper ascending central series never begins.

Moreover, whenever $q \equiv 1 \pmod{p}$, the non-abelian group of order pq is never nilpotent for the same reason. $\square$

Hint: Use the isomorphism theorems.

41 Metabelian A group G is call *metabelian* of there exists a normal subgroup N of G with N and G/N both abelian. Prove that every subgroup of a metabelian group is metabelian. Prove that every quotient of a metabelian group is metabelian.

Proof: Let $H \leq G$. Certainly $N \cap H \trianglelefteq H$ as $N \trianglelefteq G$. Moreover, N is abelian so so must be all its subgroups, including $N \cap H$. By the second isomorphism theorem we know $NH/N \cong H/N \cap H$, and as G/N is abelian, and NH/N is a subgroup of G/N, it follows NH/N is abelian; therefore, $H/N \cap H$ is abelian. Hence H is metabelian.

Let $K \trianglelefteq G$ and consider G/K. As both N and K are normal it follows NK is normal so NK/K is normal in G. Moreover, $NK/K \cong N/N \cap K$ which we know to be abelian because it is the quotient of an abelian group – namely of N. Thus G/K as a normal subgroup NK/K which is abelian. Finally, $(G/K)/(NK/K) \cong G/NK$ by the third isomorphism theorem. Yet $N \leq NK$ and G/N is abelian, so G/NK is abelian proving that indeed G/K is metabelian. $\square$

42 Normalizers of Sylow subgroups – True or False? If P is a Sylow p-subgroup of the finite group G, then $N_G(P)$ contains just one Sylow p-subgroup of G.

Hint: Sylow p-subgroups are conjugate.

Proof: If P is a Sylow p-subgroup of G, then it must also be a Sylow p-subgroup of $N_G(P)$. However it is also normal in $N_G(P)$ so it may not be conjugate to any other subgroup of $N_G(P)$. If there is another Sylow p-subgroup Q, of G, in $N_G(P)$ then it would also be a Sylow p-subgroup of $N_G(P)$ and thus it would be conjugate to P. As just stated this cannot occur so $N_G(P)$ may not contain any other Sylow p-subgroup but P itself. $\square$

43 Inherited Sylow subgroups If $H \leq G$ are finite groups, then $r_p(H) \leq r_p(G)$.

Hint: Use normalizers.

Proof: First notice we may describe the number of Sylow p-subgroups by the the counting arguments of group actions: all Sylow p-subgroups are conjugate, so $r_p(G) = [G : N_G(P)]$ for any Sylow p-subgroup P. Every Sylow p-subgroup P_H of H is a p group of G so it can be extended to a Sylow p-subgroup P_G in G. Thus $P_H = P_G \cap H$. In the same way $N_G(P_G) \cap H = N_G(H)$. Therefore

$$r_p(G) = [G : N_G(P_G)] \geq [H : N_H(P_G \cap H) = [H : N_H(P_H)] = r_p(H)$$

by the parallelogram law. $\square$

44 Normalizers of Sylow-subgroups. Let $H \leq G$ be finite groups, P be a Sylow-p-subgroup of H, and $N_G(P) \leq H$. Then P is a Sylow-p-subgroup of G.

Hint:

Proof: Suppose Q is a Sylow-p-subgroup of G containing P. Take any $g \in P$. Clearly $gPg^{-1} = P$ and as $P \leq Q$ also $gQg^{-1} = Q$ so indeed $g \in N_G(P) \cap N_G(Q)$ so that $P \leq N_G(P) \cap N_G(Q)$.**PENDING:** I don't know. $\square$

45 Simple Groups of Order pqr. If $|G| = pqr$, show that G is not simple, with p, q and r prime.

Hint: Count the number of elements required to avoid normal Sylow subgroups.

Proof: Suppose $p < q < r$. Then we know the total number of elements in G must be bounded below by

$$1 + r_p(p-1) + r_q(q-1) + r_r(r-1).$$

From the Sylow theorems we know $r_r = 1, pq$, and we focus on $r_r = pq$ since we suspect G is simple. Also $r_q = 1, r, pr$, the best case is that $r_q \geq r$. Finally for the same reasons $r_p \geq q$ as we want only a lower bound. This gives us:

$$1 + q(p-1) + r(q-1) + pq(r-1) = pqr + (qr+1) - (q+r).$$

However $q + r < qr + 1$ and so our total number exceeds the allocation of pqr many elements. So we recognize one of the Sylow subgroups is unique and thus normal; hence, G is not simple. $\square$

Hint: In the case where there is no normal p-subgroup, consider $P = \langle g \rangle$ and show that $g^i xP \neq g^j xP$ for any $x \notin P$. Then use this to show the non-p-elements all take the form $g^i x g^{-i}$.

46 Simple Groups of Order $p(p+1)$. Let $|G| = p(p+1)$, where p is prime. Show G has either a normal subgroup of order p or a normal subgroup of order $p+1$. [8]

Proof: Consider the Sylow-p-subgroups. If $r_p = 1$, then there is a normal Sylow-p-subgroup.

Now suppose instead that $r_p = p + 1$, and let P be a Sylow-p-subgroup. Given P is of prime order it is cyclic so there exists a generator $g \in P$. No take an element $x \in G$ which is not in any of the Sylow-p-subgroups. It is clear that x does not have order p.

Now we study the cosets (without making assumptions that P is normal.) If $g^i xP = g^j xP$, then $g^{i-j} xP = xP$ and even $x^{-1} g^{i-j} x \in P$. If $i \neq j$ then g^{i-j} generates P so indeed $x^{-1}Px = P$. Notice, furthermore, that $[G : N_G(P)] = p + 1$ since $r_p = p + 1$, so indeed $N_G(P) = P$. However, $g^{i-j} \in P$ and x is not, so $x^{-1}Px \neq P$. This means that $i = j$. Therefore the cosets

$$P, \quad xP, \quad gxP, \cdots, \quad g^{p-1}xP$$

are all distinct. Furthermore, as there are $p+1$ of them, they are all the cosets of P. This means the following representatives from each coset are distinct:

$$1, \quad x, \quad gxg^{-1}, \cdots, \quad g^{p-1}xg^{-(p-1)}.$$

More to the point, as x is not of order p, neither is gxg^{-1}, through $g^{p-1}xg^{-(p-1)}$, and none are trivial. Of the total $p(p+1)$ elements, $1 + (p-1)(p+1)$ of them are found in Sylow-p-subgroups leaving only p many non-p-elements. These are precisely the $g^i x g^{-i}$ elements, and each is found in one and only one coset of P.

Now we can conclude that the non-p-elements are closed under multiplication. Take x and y to be two non-trivial, non-p-elements. If xy is contained in a Sylow-p-subgroup, then without loss of generality we may assume $xy \in P$. So $y \in x^{-1}P$. Yet $x^{-1} \in P$, and certainly x^{-1} is a non-p-element. As every coset has a unique non-p-element it follows $y = x^{-1}$ so xy lies in a Sylow-p-subgroup if and only if $xy = 1$. So multiplication of non-p-elements is closed.

As such that set H of all non-p-elements is the lone subgroup of order $p+1$ so it is trivially normal.[9] $\square$

Hint: Consider the Cayley representation of G and its intersection with A_n.

47 Cyclic Sylow-2-subgroups. Let a finite group G have a cyclic Sylow-2-subgroup. Show that G has a subgroup of index 2.

Proof: Let $n = |G|$. We choose first to represent G as a permutation group under the traditional Cayley representation of left regular action. Notice then that $G \cap A_n$ is a subgroup of G which has at most index 2 – as we know

$$[G : G \cap A_n] \leq [S_n : A_n] = 2.$$

So if we can demonstrate that $G \neq A_n$ then we will be forced to conclude that $G \cap A_n$ has index 2 in G.

---

[8] This is a trivial result if it is observed that G is a Frobenius group. However, the proof that Frobenius groups are semi-direct products requires character theory and is therefore outside the nature of this chapter.

[9] Note that moreover every non-trivial element of H is conjugate, so indeed, $H \cong C_q \times \cdots \times C_q$ for some prime q and in fact this occurs if and only if $p + 1 = q^i$ for some prime q.

As $n = |G|$ we take $n = 2^k m$ with $(2, m) = 1$. We are given that G has a cyclic Sylow-2-subgroup, so we may say it is generated by an element g of order 2^k. Hence under the regular representation we find g is represented by

$$(h_1, gh_1, g^2h_1, \dots, g^{2^k-1}h_1) \cdots (h_m, gh_m, g^2h_m, \dots, g^{2^k-1}h_m)$$

where the h_i's are a transversal for the cosets of $\langle g \rangle$. Each of these cycles has even length so it follows as permutations they are odd permutations, and as m is also odd, the total sign of our permutation representation of g is odd times odd which is odd. Hence G contains an odd element, namely the regular representation of g, and as such it follows $G \neq A_n$. □

48 Automorphism of S_n. Let $n \neq 6$. Then every automorphism of S_n is inner.

Hint:

Proof: Let $f : S_n \to S_n$ be an automorphism of S_n, for $n \neq 6$. We know f must send conjugate subgroups to conjugate subgroups as

$$f(gHg^{-1}) = f(g)f(H)f(g)^{-1}.$$

We know that the stabilizers of points, $1, \dots, n$, are all conjugate as they are stabilizers of the same action – namely S_n acting on $1, \dots, n$. Denote $Stab_{S_n}(k)$ by S_{n-1}^k and notice they are isomorphic to S_{n-1} for each $k = 1, \dots, n$. It follows any automorphism of S_n is therefore a permutation on the S_{n-1}^k subgroups. □

49 Automorphism of S_6. The group S_6 has an automorphism mapping the stabilizer of a point in S_6 to a transitive subgroup. No such automorphism can be inner.

Hint:

Example:

□

50 Nilpotency and Normalizers. Let G be a finite group. Then G is nilpotent if and only if H is a proper subgroup of $N_G(H)$, whenever H is a proper subgroup of G.

Hint: The normalizer of a product is the product of the normalizers.

Proof: Suppose G is nilpotent, then it is is the direct product of it Sylow p-subgroups; say $G = P_1 \times \cdots \times P_n$. Now take H a proper subgroup of G. Since there is a unique Sylow p-subgroup for each p dividing the order of G, it follows $H = H \cap P_1 \times \cdots \times H \cap P_n$. Now it follows

$$N_G(H) = N_G(H \cap P_1) \times \cdots \times N_G(N \cap P_n).$$

If each $N_G(H \cap P_i) = H \cap P_i$ then $H = G$ because the normalizer of a proper subgroup of any Sylow p-subgroup will be at least P and when G is nilpotent G. Thus H is strictly contained in $N_G(H)$.

In the converse take any Sylow p-subgroup P_i. Then if $G = P_i$ it is nilpotent. If not then P_i is proper so $N_G(P_i) \neq P_i$. However we know for Sylow p-subgroups that $N_G(N_G(P_i)) = N_G(P_i)$ so the only case this can occur is when $N_G(P_i) = G$. Therefore each Sylow subgroup is normal in G so G is nilpotent. □

51 Dihedral Nilpotency. – True or False? D_{2n} is nilpotent.

Hint: Note that $D_{4n}/Z(D_{4n}) \cong D_{2n}$.

Lemma 1.0.3 $D_{2in}/\langle a^i \rangle \cong D_{2n}$.

Proof: Since $\langle a\rangle$ is a cyclic normal subgroup, all its subgroups are normal. Therefore $\langle a^i\rangle$ is normal. Notice, $\langle a^i\rangle$ has index n in $\langle a\rangle$; therefore, $a\langle a^i\rangle$ has order n. Likewise, $b\langle a^i\rangle$ has order 2. Since $\langle a^i\rangle$ has index $2n$ in D_{2n}, it follows $D_{2in}/\langle a^i\rangle$ has order $2n$. Finally,

$$b\langle a^i\rangle a\langle a^i\rangle = ba\langle a^i\rangle = a^{-1}b\langle a^i\rangle = a^{-1}\langle a^i\rangle b\langle a^i\rangle.$$

Therefore $D_{2in}/\langle a^i\rangle \cong D_{2n}$ since it has the same presentation of the dihedral group D_{2n}. □

Theorem 1.0.4 *D_{2n} is nilpotent if and only if $n = 2^k$ for some k.*

Proof: If $n = 1 = 2^0$ then D_{2n} is C_2 which is nilpotent; likewise when $n = 2$, D_{2n} is abelian so it is nilpotent. Now consider $n > 2$.

From Exercise-1.77 we know the center of D_{2n} is trivial if and only if n is odd. So if n has any odd factors we use the above lemma to quotient out the centers and arrive at D_{2m} where $(2, m) = 1$. Here the center is finally trivial so the ascending central series does not terminate with the whole group so it is not nilpotent. Whenever n has no odd factors it is a 2-group so it is nilpotent. □

Hint: Use the first isomorphism theorem.

52 Sylow-subgroups of Quotients. Let $\varphi : G \to H$ be a surjective homomorphism of finite groups. If P is a Sylow-p-subgroup of G, then $\varphi(P)$ is a Sylow-p-subgroup of H. Conversely, every Sylow-p-subgroup of H is the image of a certain Sylow-p-subgroup of G.

Proof: Take $K = Ker\ \varphi$. Let $|P| = p^n$. By the parallelogram law we know $[PK : K] = [P : P \cap K] = p^i$. Hence PK/K is a p-subgroup of G/K. Also, $i = [G/K : PK/K] = [G : PK]$ but as P is a Sylow-p-subgroup in G, it follows $(i, p) = 1$. Thus, PK/K is indeed a Sylow-p-subgroup of G/K. By the first isomorphism theorem we see in fact $\varphi(P)$ is a Sylow-p-subgroup of H.

Now take Q a Sylow-p-subgroup of H. It follows $K \le \varphi^{-1}(Q)$. Now take P to be a Sylow-p-subgroup of $\varphi^{-1}(Q)$. If P is not a Sylow-p-subgroup of G, then there exists some Sylow-p-subgroup P' containing P. Such a subgroup also contains K, and so $p^j = [P' : K] > [P : K] = p^i$ with $i < j$. However, this produces a strictly large p-subgroup in the quotient space G/K. This applies to H by the first isomorphism theorem so indeed such a P' cannot exist. Therefore P is a Sylow-p-subgroup of G and $\varphi(P) = Q$. □

Hint: Use conjugation of Sylow-p-subgroups prove $P \cap N$ is Sylow in N.

53 Sylow-subgroups of Normal subgroups. Let G be a finite group, $N \trianglelefteq G$, and P a Sylow-p-subgroup of G for some prime p. Show that PN/N is a Sylow-p-subgroup of G/N and $P \cap N$ is a Sylow-p-subgroup of N.

Proof: Take $\varphi : G \to G/N$ to be the canonical projection. Now make use of Exercise-1.52 to conclude that PN/N is Sylow-p-subgroup of G/N. That $P \cap N$ is a Sylow-p-subgroup of N follows with a little more care.

Suppose Q is a Sylow-p-subgroup of N containing $P \cap N$. Then Q is contained in some Sylow-p-subgroup of G, call it P'. Thus P and P' are conjugate, say by g. Hence:

$$gP \cap Ng^{-1} = gPg^{-1}g \cap Ng^{-1} = P' \cap N = Q.$$

Thus $|Q| = |P \cap N|$ which means $Q = P \cap N$ so indeed $P \cap N$ is a Sylow-p-subgroup of N. □

Hint: Act on the order conjugacy class.

54 Conjugacy Classes. If a group G contains an element having exactly two conjugates, then G has a non-trivial proper normal subgroup.

Proof: Let $X = \{a, b\}$ be the given conjugacy class of order 2. Note that G acts transitively on X by conjugation. This induces a natural surjection $G \to S_2$ proving G has a normal kernel of index 2. Thus $G = C_2$, or the subgroup is a proper non-trivial normal subgroup. If $G = C_2$ then there is no conjugacy class of order 2. $\square$

55 Embedding in A_n. Any finite group is isomorphic to a subgroup of A_n for some n.

Hint: Attach a transposition to any odd permutations.

Proof: By Cayley's theorem we know the right regular action of G induces a natural embedding of G in S_n, via σ_g, where $n = |G|$. The generalization to A_{n+2} is possible with the following construction.

Define $f : G \to A_{n+2}$ as $f(g) = \sigma_g$ if σ_g is an even permutation. In the case that σ_g is an odd permutation, it follows that some cycle in a disjoint cycle decomposition of σ_g is of even length, or σ_g is a product of disjoint transpositions. In any event, the order of σ_g is even. As such we may assign $f(g) = \sigma_g(n + 1, n + 2)$. As $n + 1$ and $n + 2$ are fixed by S_n, this addition does not interfere with the embedding and simply serves to make each permutation even. $\square$

56 C_{15} as a Permutation Group. – True or False? A_5 contains no subgroup of order 15.[10]

Hint: Act on the cosets of such a subgroup.

Proof: Suppose H is a subgroup of order A_5. Since $[A_5 : H] = 4$, it follows A_5 acts on 4 elements transitively so A_5 embeds in S_4. However $|A_5| = 60$ and $|S_4| = 24$ which means there is a proper non-trivial kernel in A_5. Yet A_5 is simple so no suitable kernel exists. $\square$

57 C_{15} as a Permutation Group. Find the smallest n such that A_n contains a subgroup of order 15.

Hint: The only group of order 15 is C_{15} and such a subgroup does not embed in S_n until S_8.

Example: $n = 8$ is required. To see, this first we recall that the groups of order pq are classified. As $5 \not\equiv 1 \pmod 3$ it follows the only group of order $3 \cdot 5$ is C_{15}. To build a permutation of order 15 requires one of two things: a cycle of length 15, or a disjoint product of a 3 cycle and a 5 cycle. Thus we need at least $n = 8$.

When $n = 8$ the element $(123)(45678)$ has order 15 and is even so indeed we have C_{15} embedded in A_8. $\square$

58 Normal Sylow-subgroups. – True or False? Let G be a finite group, and let P be its Sylow-p-subgroup. If $P \trianglelefteq N \trianglelefteq G$ then $P \trianglelefteq G$.

Hint: Note all Sylow-p-subgroups are hence contained in N (Exercise-1.53).

Proof: As P is Sylow G, and contained in N, it must be a Sylow-p-subgroup of N as well. We know given any Sylow-p-subgroup Q, $Q \cap N$ is a Sylow-p-subgroup of N by Exercise-1.53. This means every Sylow-p-subgroup of G is completely contained in N or otherwise the intersection would be of an order less than that of P. However now we see that since P is normal in N it cannot be conjugate to any other subgroups of N, so N must have a unique Sylow-p-subgroup, and so indeed G has a unique Sylow-p-subgroup proving P is normal in G. $\square$

59 Centers of p-groups. Let G be a finite p-group, and $N \trianglelefteq G$ be a normal subgroup of order p. Then N is in the center of G.

Hint: Consider the size of a conjugacy class in N.

[10] The only group of order 15 is cyclic, and clearly now permutation on 5 letters can have order 15. So such a subgroup is not in S_5 much less A_5.

Proof: Take any element $n \in N$. If N is not central then there is an element $g \in G$ which conjugates n non-trivially. If $gng^{-1} \notin N$ then N is not normal. Thus $gng^{-1} \in N$. This means that the conjugacy class of n is contained entirely in a group of order p. If $n = 1$ then the class has order 1. Thus if $n \neq 1$ then its conjugacy class has order less than or equal to $p - 1$. However all numbers less than p are relatively prime to p, and so as all conjugacy classes must have order dividing that of the group, the conjugacy class of n must be 1. Hence n is central so $N \leq Z(G)$. □

Hint: Every p-group is nilpotent.

60 Centers. If G is a finite p-group, $N \trianglelefteq G$, and $N \neq \mathbf{1}$, then $N \cap Z(G) \neq \mathbf{1}$.

Proof: First we know from Prop-1.9.21 every p-group is nilpotent. When we combine this with Prop-1.9.25 we have every non-trivial normal subgroup of G intersects the center non-trivially. □

Hint: Look at commutators between the product.

61 Centers of Products. Let H, K, N be non-trivial normal subgroups of a group G, and suppose that $G = H \times K$. Prove that N is in the center of G or N intersects H, K non-trivially. Give an example where N is in the center and does not intersect either H or K non-trivially. Give an example where N is not in the center but intersects both H and K non-trivially. Give an example when N is in the center and intersects both H and K non-trivially.

Proof: Suppose $H \cap N = K \cap N = \mathbf{1}$. Take a commutator from each: let $h \in H$, $k \in K$ and $n \in N$; then $[h, n] \in N$ as N is normal, and also $[h, n] \in H$ as H is normal, so $[h, n] = 1$ as their intersection is trivial. The same goes for $[k, n]$. Therefore N is central to all elements of H and to all elements of K, so since $HK = G$ it follows N is central to all elements in G, so $N \leq Z(G)$. □

Example: $D_2 = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ [11] has a normal subgroup $\langle ab \rangle$ which does not intersect either product. However since the group is abelian every thing is contained in the center.

In D_6 the center is no longer the entire group but simply $\langle a^3 \rangle$ (see Exercise-**??**). $\langle a^3 \rangle, \langle a^2, b \rangle \trianglelefteq D_6$ and nontrivial. $\langle a^3 \rangle \cap \langle a^2, b \rangle = \mathbf{0}$ and finally $\langle \langle a^3 \rangle \cup \langle a^2, b \rangle \rangle = \langle a^2, a^3, b \rangle = D_6$. Therefore $D_6 = \langle a^3 \rangle \times \langle a^2, b \rangle \cong \mathbb{Z}_2 \times D_3$. [12]

The list of nontrivial normal subgroups of D_6 is (Exercise-**??**):

$$\langle a^3 \rangle, \langle a^2 \rangle, \langle a \rangle, \langle a^2, b \rangle, \langle a^2, ab \rangle.$$

Clearly the first non-trivially intersects $\langle a^3 \rangle$ – and it is contained in the center (it is the center); the next four non-trivially intersect $\langle a^2, b \rangle$ – they all contain $\langle a^2 \rangle$. □

Hint: Each is false.

62 Counter Examples. – True or False? For $i = 1, 2$ let $H_i \trianglelefteq G_i$, determine which are true and which are false.

(a) $G_1 \cong G_2$ and $H_1 \cong H_2 \Rightarrow G_1/H_1 \cong G_2/H_2$.

(b) $G_1 \cong G_2$ and $G_1/H_1 \cong G_2/H_2 \Rightarrow H_1 \cong H_2$.

(c) $H_1 \cong H_2$ and $G_1/H_1 \cong G_2/H_2 \Rightarrow G_1 \cong G_2$.

Example:

(a) $\mathbb{Z} \cong \mathbb{Z}$ and $2\mathbb{Z} \cong \mathbb{Z} \cong 3\mathbb{Z}$ but certainly $\mathbb{Z}/2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/3\mathbb{Z}$ as they do not even have the same order.

[11] D_2 is the symmetries of a rectangle.

[12] D_6 is the symmetries of a hexagon, which contains two disjoint regular triangles whose symmetries are D_3 – hence D_6 is structurally equivalent to a product of D_3.

(b) $D_8 \cong D_8$ and $D_8/\langle a\rangle \cong \mathbb{Z}_2 \cong D_8/\langle a^2, b\rangle$ but $\langle a\rangle$ is cyclic and $\langle a^2, b\rangle$ is not, so they are not isomorphic.

(c) $\langle 2\rangle \trianglelefteq \mathbb{Z}_4$ and $\langle (1,0)\rangle \trianglelefteq \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Notice $\langle 2\rangle \cong \mathbb{Z}_2 \cong \langle (1,0)\rangle$, and $\mathbb{Z}_4/\langle 2\rangle \cong \mathbb{Z}_2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2/\langle (1,0)\rangle$; however, $\mathbb{Z}_4$ is cyclic while $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not, so they are not isomorphic.

□

63 Solvable Groups. Let G be a finite group. If G is solvable, then G contains a non-trivial normal abelian subgroup. If G is not solvable then it contains a normal subgroup H such that $H' = H$.

Hint: Consider the last term in the derived series.

Proof: Consider the derived series of G. First notice $G^{(i)}$ is normal in G for all i. In the first case G' is normal. Now suppose $G^{(i)}$ is normal in G. Then taking any generator $[a,b] \in G^{(i+1)}$ and any $x \in G$, it follows $a, b \in G^{(i)}$ so $xax^{-1}, xbx^{-1} \in G^{(i)}$ since $G^{(i)}$ is normal. Moreover now we see:

$$x[a,b]x^{-1} = xaba^{-1}b^{-1}x^{-1} = xax^{-1}xbx^{-1}xa^{-1}x^{-1}xbx^{-1} = [xax^{-1}, xbx^{-1}].$$

Since $G^{(i+1)}$ contains all commutators of $G^{(i)}$ it must therefore contain $x[a,b]x^{-1}$. Since $G^{(i+1)}$ is closed under conjugation of generators it is in fact closed to conjugation of all elements. Therefore $G^{(i+1)}$ is normal in G so by induction the derived series is a normal series.

If G is solvable then the series must terminate at some n. Thus the commutator of $G^{(n-1)}$ is trivial. Therefore $G^{(n-1)}$ is abelian and thus G has a normal abelian subgroup.

If G is not solvable, then the series must not terminate. However the group is finite so the sequence must stabilize at some $G^{(n)}$; that is: $(G^{(n)})' = G^{(n)}$ for some n and $G^{(n)} \neq \mathbf{1}$. □

64 Subgroups of $C_p \times C_p$. Let p be prime. Show the number of subgroups of $C_p \times C_p$ is $p + 3$.

Hint: Number of generator in each copy of C_p is $p - 1$.

Proof: Given any $(a,b) \in C_p \times C_p$ it follows $(a,b)^p = (a^p, b^p) = (1,1)$. Thus every non-trivial element generates a subgroup of order p. Furthermore, each such subgroup contains $p-1$ non-trivial elements. Since every proper subgroup of $C_p \times C_p$ must have order p, it follows this counts all proper subgroups. There are, therefore, $p^2 - 1$ elements in proper subgroups of $C_p \times C_p$ each which contains $p - 1$ elements for a total of $\frac{p^2-1}{p-1} = p + 1$ proper subgroups. Adding the two trivial groups we get our formula. □

65 Automorphisms. Let G be a group, and suppose $|Aut(G)| = 1$. Prove that G has at most two elements.

Hint: Treat in cases: G non-abelian, abelian, and G as a group of involutions.

Proof: If G is non-abelian then there exists elements $g, h \in G$ such that $gh \neq hg$ so indeed $ghg^{-1} \neq h$. However conjugation is always an automorphism of G, so we are now convinced there is a non-trivial automorphism of G.

Now suppose G is abelian.

If G has an element that is not of order 2, then the automorphism $f(x) = -x$ is non-trivial. We see this is indeed an automorphism since it is clearly bijective – inverses are unique – and as G is abelian

$$f(x + y) = -(x + y) = -x + -y = f(x) + f(y).$$

Now consider the case where G is a group of involutions. As G is still abelian, $\mathbb{Z}$ acts on G but $2\mathbb{Z}$ annihilates G so indeed G is a $\mathbb{Z}_2$ vector space. Thus

$$G \cong \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2 = \mathbb{F}_2^n.$$

Thus G has $GL_n(\mathbb{F}_2)$ as its automorphism group which is non-trivial unless $n = 1$. Therefore $|Aut(G)| > 1$ unless $|G| \leq 2$. □

Hint: Consider the dihedral groups.

66 Nilpotency of order 18. – True or False? Every group of order 18 is nilpotent.

Example: False. In Exercise-1.51 we saw D_n was nilpotent only if n was a power of 2. Hence D_{18} is not nilpotent and it is a group of order 18. □

Hint: Consider $C_2 \times C_2$.

67 Diagonal Embedding. Let G_1, and G_2 be finite groups. Is it true that every subgroup of $G_1 \times G_2$ is of the form $H_1 \times H_2$, where $H_1 \leq G_1$ and $H_2 \leq G_2$? What if additionally $(|G_1|, |G_2|) = 1$?

Example: The first assumption is false. We see this even with the smallest example $C_2 \times C_2$. Here the subgroup $\langle(1, 1)\rangle$ is isomorphic to C_2 but its left and right projections are C_2, suggesting it should be $C_2 \times C_2$, which it is not. Therefore the subgroup cannot be split. □

However adding the condition of relatively prime is sufficient. **Proof:** Suppose $|G_1|$ and $|G_2|$ are relatively prime. Let $H \leq G_1 \times G_2$. If we take any $(h_1, h_2) \in H$ we observe the following:

$$(h_1, h_2)^{|G_1|} = (1, h_2^{|G_1|}) = (1, h_2').$$

Since the order of $|G_1|$ is relatively prime to $|G_2|$ it must also be relatively prime the order of any element h_2 in G_2; thus, h_2' has the same order as h_2 and moreover generates h_2 – say by a power k. Therefore:

$$(h_1, h_2)^{|G_1|k} = (1, h_2'^k) = (1, h_2).$$

Therefore, $\pi_2(H)$ is naturally embedded in H as $\mathbf{1} \times \pi_2(H)$. The same goes for $\pi_1(H)$.

Clearly $H_1 = \pi_1(H) \times \mathbf{1}$ and $H_2 = \mathbf{1} \times \pi_2(H)$ split in H, and they are normal in H because they are equivalent to $G_1 \cap H$ and $G_2 \cap H$ and we know both G_1 and G_2 are normal. Therefore H is the internal direct product of H_1 and H_2. □

Hint: Consider D_8.

68 Centrality in p-groups. – True or False? Any element of order p in a finite p-group is central.

Example: In D_8 every flip is of order 2, yet no flip is central. □

Hint: Consider the action of G on the cosets of H.

69 Classification of Sylow-subgroups. Let p be a prime and G be a finite simple group having a subgroup H of index p. Find the isomorphism type of a Sylow-p-subgroup of G.

Proof: Since G acts transitively on the subgroup's cosets we have a map $G \to S_p$. However G is simple so it is contained in A_p. Now we see that the order of G is less than or equal to $p!/2$. This means $p|G$ but $p^2 \nmid G$ and that p (and p is the largest prime dividing the order of G.) Now we know that a Sylow-p-subgroup has order p so it is simply C_p. □

Hint: Use Sylow theory.

70 Groups of order 175. Classify the groups of order 175.

Proof: Note that $175 = 5^2 \cdot 7$; thus, the third Sylow theorem tells us there is precisely one Sylow 7-subgroup, of order 7, and is consequently normal. At the same time, since $7 \not\equiv 1 \pmod 5$ we know the number of Sylow-5-subgroups is 1 as well. Hence G has two normal subgroups that intersect trivially because their orders are relatively prime, and whose product is the entire group. So G is a direct product of its Sylow subgroups. Therefore using the classification of the groups of order p^2 we may say with certainty the groups of order 175 are

$$C_7 \times C_{25}, \qquad C_7 \times C_5 \times C_5.$$

□

71 Free-Abelian Groups. Let F be a free group with basis $X = \{x_1, \dots, x_n\}$. Then $F/F' \cong \mathbb{Z} \oplus \cdots \mathbb{Z}$, n-copies.

Proof: Define $f : F/F' \to \mathbb{Z}^n$ by $f(x_i F') = e_i$ where $\{e_1, \dots, e_n\}$ is the standard basis of the free-abelian group $\mathbb{Z}^n$. Since F/F' is abelian, the relations commutative relation holds across f so by v. Dyck's theorem we know f is a homomorphism. Moreover, $\{e_1, \dots, e_n\}$ spans $\mathbb{Z}^n$ so indeed f is surjective. Finally suppose $f(aF') = \vec{0}$. As F is free we may take a to be generated from the basis so that:

$$aF' = x_{i_1} \cdots x_{i_j} F' = x_1^{d_1} \cdots x_n^{d_n} F'$$

for appropriate i_k's and d_i's – with the last step made possible by the commutator relations in F'. As such we have

$$\vec{0} = f(aF') = f(x_1^{d_1} \cdots x_n^{d_n} F') = f(x_1^{d_1} F' \cdots x_n^{d_n} F') = d_1 e_1 + \cdots + d_n e_n$$

However $\mathbb{Z}^n$ is a free-abelian group so the e_i's are linearly independent so that their sum is 0 only if each coefficient is 0; thus, $d_i = 0$ for all i. Now we pull this result back to say

$$aF' = x_1^0 \cdots x_n^0 F' = F'.$$

Hence the kernel is trivial so our homomorphism is an isomorphism. □

Hint: Recall a basis of a free-abelian group is linearly independent.

72 Free Groups. Let $X \subseteq Y$. Show $F(X) \leq F(Y)$.

Proof: We make use of the canonical embedding:

$$\begin{tikzcd} X \arrow[r, hook, "i"] \arrow[d, hook, "\iota_X"] & Y \arrow[d, hook, "\iota_Y"] \\ F(x) \arrow[r, Rightarrow, "f"] & F(Y). \end{tikzcd}$$

f is given by applying the universal property on $F(x)$ with the map $\iota_Y i$. Now we verify that f is injective.

$$\begin{aligned} 1 &= f(\iota_X(x_{i_1}) \cdots \iota_X(x_{i_m})) \\ &= \iota_Y(i(x_{i_1})) \cdots \iota_Y(i(x_{i_m})) \\ &= \iota_Y(x_{i_1}) \cdots \iota_Y(x_{i_m}). \end{aligned}$$

Now recall that the image lies in $F(Y)$ which is free of all but the necessary group relations. Thus

$$1 = \iota_Y(x_{i_1}) \cdots \iota_Y(x_{i_m})$$

only if there is a path to reduce the letters to the empty string. This path depends only on the arrangement of the indices i_k. So we pull this path back to $F(X)$ and find it too reduces

$$\iota_X(x_{i_1}) \cdots \iota_X(x_{i_m}) = 1.$$

Thus the kernel is trivial. □

Hint: Use the universal property of $F(X)$ to create a natural injection.

Hint: The axe either through opposing verte ter of the tetra

73 Symmetries of the Tetrahedron. Find the group of rotations and the full group of symmetries of a regular tetrahedron.

Example: There are four vertices on the regular tetrahedron so the action on the vertices being sufficient to describe the symmetries tells us the symmetries lie in S_4. When we fix an axis of rotation through the center of a fact and the opposing vertex we see a rotation of order 3, so we attain all 3 cycles and thus a copy of A_4 – as the 3-cycles generate A_n in S_n. This is thus the group of rotations as it includes the rotations $(ab)(cd)$ which are those whose axis of symmetry is the center of the tetrahedron.

For the full group of symmetries we must convince ourselves that there are no other symmetries. If we add any odd permutation we will acquire all of S_4 as our symmetries. Thus consider a permutation (ab). If two adjacent vertices are fixed then the edge between them is fixed and thus the triangles that share this edge are fixed. This means two of the 4 triangle faces are fixed, and thus the edges of these triangles are also fixed. This means indeed all the triangles are fixed as the two triangles already fixed share two edges with the remaining two triangles. Finally, unlike the cube, any two vertices are adjacent so this is always the case. Hence, the symmetries do not contain a permutation of the form (ab) so they cannot be all of S_4. Since they must contain A_4 – the group of all rotations – we are forced to conclude the full symmetry group is precisely the group of rotations: A_4. □

Hint: Permutations in S_n are conjugate if they have the same cycle structure.

74 Conjugation in S_5. Describe the conjugacy class of A_5 and S_5.

Example: In S_n permutation with the same cycle structure are conjugate. So in S_5 we have the following conjugacy classes: (let a, b, c, d, e be distinct elements from $\{1, 2, 3, 4, 5\}$)

$$[()], \quad [(a,b)], \quad [(a,b,c)], \quad [(a,b,c,d)], \quad [(a,b)(c,d)],$$
$$[(a,b,c,d,e)], \quad [(a,b,c)(d,e)],$$

with respective orders: $1, 10, 20, 30, 15, 24, 20$.[13] The sum is 120 so we have accounted for all the permutations.

Now in A_n we are not privileged to have as strong a statement as we have in S_n. First of all the size of the conjugacy classes must divide the order of the group, so we can only select from 1,2,3,4,5,6, 10, 12, 15, 20, 24, or 30. To help us narrow the study consider any class order less than 5. Then conjugation acts transitively on this class so that we require a homomorphism $A_5 \to S_k$, with $k < 5$. Since A_5 is simple this requires the action to be trivial – which it is not unless the class is of order 1. However the center of A_5 is trivial so the only class of order less than 5 is $[()]$. These leaves us with the possible orders 5,6, 10, 12, 15, 20, 24, and 30. Note moreover that this applies not only to the size of conjugacy classes of elements but also of subgroups.

We observe that in A_4, the permutations $(a,b)(c,d)$ are all conjugate – for instance by (a,b,c) we see it is conjugate to $(a,d)(b,c)$ and from (a,c,b) we get $(a,c)(b,d)$. Now we put this to use. As $(a,b)(c,d)$ fixes e, it must be in A_4^e which is the copy of A_4 in A_5 which fixes e. Hence all copies of A_4 in A_5 have disjoint 2 by 2 cycles. By the above reasoning we know that the subgroups A_4^i

[13] The number of cycles of length r from n letters is given by

$$nJr = \frac{n!}{(n-r)!r}.$$

For k disjoint copies of length r from n letters simply notice this is produced from a cycle of length kr taken to the r/k power.

(of which there are five because we can only fix one of the five letters at a time) are conjugate. Therefore indeed the conjugation extends to the 2 by 2 cycles so we may now conclude that all 2 by 2 cycles are conjugate in A_5.

Now we are left with 3 cycles and 5 cycles. We must partition the total 20 3-cycles and 24 5-cycles into conjugacy classes whose orders are 5, 6, 10, 12, 15, 20, 24, 30. In A_4 the 3-cycles break into 2 conjugacy classes each of size 4, since the the elements are not central, 8 does not divide 12, and there is no subgroup of index 2 so there is no centralizer of this order. Thus in A_5 the 3-cycles are at least in classes of size 4. However the A_4^i subgroups are conjugate so we must extend this conjugation to the classes in A_4 to see that we either connect them all into 2 classes, or into 1. However we notice the centralizer of (a, b, c) is contains (a, b, c) and (d, e) so it must have order at least 6 which forces use to conclude the class size is no larger than 10. Yet it must be exactly 10 so that there are only 2 classes.

This also tells us about $(a, b, c)(d, e)$. Since the first component is conjugate only in groups of 10, then we must have these conjugate in groups of 10 or 5. If it is 5 then the centralizer must have order 12 which would make it A_4 (no other order 12 group lies in A_5). Yet the centralizer must contain the element which would mean A_4 has an element of order 6 which it does not. So the elements $(a, b, c)(d, e)$ are arranged in two classes of order 10 each.

Finally, the 30 5-cycles must be arranged. The centralizer must have order at least 5 which requires the classes have order no greater than 12. This means either 2 classes of order 12, or 4 classes of order 6, etc – we know the arrangement to be homogeneous because all centralizers are conjugate and so the their indices are equal. If it is 6 then we require the copy of D_{10} in A_5 centralizer its 5-cycles – which it does not – the center of D_{10} is trivial. Hence it must be 12 as the centralizer must be C_5.

So the conjugacy classes of A_5 are: a single $[()]$ of order 1, 2 classes of 3-cycles, each of order 10, 1 class of 2 by 2 cycles, and of order 15, 2 classes of order 10 of 3 by 2 cycles, and 2 classes of order 12 each of 5-cycles. □

75 Dihedral Groups. – True or False? $D_{12} \cong S_3 \times C_2$.

Hint: Consider the regular triangles embedded in a regular hexagon.

Proof: Geometrically the proof is simple: the hexagon has two regular triangles inscribed within. This gives two copies of $D_6 \cong S_3$ in D_{12}, both of index 2 so they are normal. Now consider the rotation a^3 which visibly has order 2. This rotates one regular triangle onto the other. In particular this tells us it does not intersect the copies of D_6. As $a^3 b = ba^3$ we see a^3 is central so this C_2 subgroup is normal. Hence we have two normal subgroups that intersect trivially and whose join is the entire group. Hence we have an internal direct product so indeed: $D_{12} \cong D_6 \times C_2$. □

76 S_p generators. Let p be prime g be any p-cycle in S_p and h be any transposition in S_p. Prove $\langle g, h\rangle = S_p$.

Hint: Show that all transposition can be determined from the cycle. Make sure to use the primality of p.

Proof: Take $\sigma = (a_0, \ldots, a_{p-1})$ and $\tau = (a_0, a_i)$ (we can rotate the numbers in σ so that the first terms agree, thus choice imposes nothing outside the hypothesis). We also know

$$\sigma^j \tau \sigma^{-j} = (a_{\sigma^j(1)}, a_{\sigma^j(i)})$$

where $i + 1$ i modulo p. Since p is prime we know the cycles remain the same length as we take powers:

$$\sigma^j = (a_1, a_j, a_{2j}, \ldots).$$

Together we see we can construct the transpositions:

$$(a_0, a_i), (a_1, a_{i+1}), \ldots, (a_{p-1}, a_{i+p-1})$$

Since we have p distinct transpositions so they generate a symmetric group. Yet we also have that they are transitive on all p elements so they must generate S_p. $\square$

77 Dihedral Groups. Let D_{2n} be the dihedral group of order $2n$. For which values of n:

(a) The center of D_{2n} is trivial?

(b) All involutions in D_{2n} are conjugate to each other?

(c) D_{2n} is a direct product of two proper subgroups?

(a) **Proposition 1.0.5** *Let $n > 2$. If n is even then the center of D_{2n} is $\langle a^{n/2}\rangle$, and when n is odd the center is trivial.*

Remark 1.0.6 *When $n = 2$, D_{2n} is simply the Klein 4-group $C_2 \times C_2$ which will have as its center all of D_{2n}. When $n = 1$, $D_2 \cong C_2$ so we restrict our attention to $n > 2$.*

Proof: To see this we make use of the free presentation:

$$D_{2n} = \langle a, b \mid a^n = b^2 = e, ba = a^{-1}b\rangle$$

and D_{2n} has order $2n$. Notice this last relation gives D_{2n} the normal form $a^i b^j$.

Suppose $a^i b$ is central; then given any a^k it should follow:

$$a^{i-k}b = (a^i b)a^k = a^k(a^i b^j) = a^{i+k}b.$$

However this implies $a^{-k} = a^k$ for all $k = 1, \ldots, n$. Since $n > 2$ this will not be true for all k. Therefore the center of D_{2n} may not contain an element of the form $a^i b$.

Suppose a^i is central. Then for all $a^j b$ it follows:

$$a^{i+j}b = a^i(a^j b) = (a^j b)a^i = a^{j-i}b,$$

which requires $a^{j+i} = a^{j-i}$ or simply that $a^i = a^{-i}$. Of course this requires $2|n$ and that $i = n/2$. Now we check; let $2|n$, then:

$$a^{n/2}(a^j b) = a^{n/2+j}b = a^j a^{n/2}b = a^j ba^{-n/2} = (a^j b)a^{n/2}.$$

Since a^i is clearly central to all a^j we may conclude the center of D_{2n} is $\langle a^{n/2}\rangle$ when n is even and trivial otherwise. $\square$

(b) **Proposition 1.0.7** *Let $n > 2$. If n is even then the involutions break into conjugacy classes of:*

$$\{a^{n/2}\}, \{b, a^2 b, \ldots, a^{n-2}b\}, \{ab, a^3 b, \ldots, a^{n-1}, b\}.$$

If n is odd then we have all involutions conjugate to each other.

Proof: We saw above that when n is even, $a^{n/2}$ is central. Hence it is in its own conjugacy class. For the rest, when we conjugate we get:

$$a^i b a^{-i} = a^{2i}; \qquad a^i (ab) a^{-i} = a^{2i} ab = a^{2i+1} b.$$

Hence we have the above conjugacy classes when n is even. When n is odd we see that $2i$ will eventually span all of $\mathbb{Z}_p$ so indeed the class becomes all involutions. □

(c) **Proposition 1.0.8** *Given* $(2, m) = 1$ *and* $n \geq 1$, *it follows*

$$D_{4m} \cong D_{2m} \times C_2.$$

Otherwise D_{2n} *does not split as a non-trivial direct product.*

Proof: Take $D_{2n} = H \times K$ for subgroups H and K of D_{2n}. As such both must be normal subgroups of D_{2n}. This means they are either subgroups of the full rotation group or they are of index 2 – since all subgroups of D_{2n} are copies of D_{2i} and are conjugate unless the index is 2. If both H and K are rotation groups then their join will not be all of D_{2n} so one must be a copy of $D_{2\frac{n}{2}}$ which requires furthermore that $2|n$. As such we now see the other group must have order 2, and so it must be C_2 and so it is the center of D_{2n} as it is the only normal involution group. In the end we see that the intersection of $D_{2\frac{n}{2}}$ and $Z(D_{2n})$ is trivial only when $\frac{n}{2}$ is relatively prime to 2. So we conclude that $n = 2m$ with $(2, m) = 1$.

Now suppose these conditions are met: $Z(D_{4m})$ intersect D_{2m} is trivial and their join is all of D_{4m}. Moreover both are normal so indeed D_{2n} is the internal direct product of these two groups. □

Chapter 2

Fields

---

1 Galois Group Order. – True or False? The Galois group of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ has order 3.

Hint: Find the degree of the minimal polynomial.

Proof: True. We notice $\sqrt[3]{2}$ is a root of x^3-2, and

$$x^3-2=(x-\sqrt[3]{2})(x^2)$$

so $irr(\mathbb{Q};\sqrt[3]{2})=x^3-2$. The minimal polynomial x^3-2 tells us the degree of the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is 3. Therefore the order of the Galois group is 3. □

2 Countable Extensions. If the extension K/k is algebraic and k is countable then K is also countable.

Hint: Note that a countable union of countable sets is countable.

Proof: Since k is countable, the ring $k[x]$ is countable as it is in one-to-one correspondence with the countable union $\bigcup_{i\in\mathbb{N}} k^i$ of countable sets. Thus there are a countable number of roots as each element in $k[x]$ has only finitely many roots. Since K is algebraic of k, every element in K is a root of some polynomial in $k[x]$ so it is a subset of the countable number of all roots of k. □

3 Countability of $\mathbb{A}$. The field $\mathbb{A}$ – all algebraic elements over $\mathbb{Q}$ – is countable.

Hint: Use Exercise-2.2.

Proof: Since $\mathbb{Q}$ is countable and by definition $\mathbb{A}/\mathbb{Q}$ is an algebraic extension, it follows from Exercise-2.2 that $\mathbb{A}$ is countable. □

4 Algebraic Towers. – True or False? If $F/K/k$ are field extensions with F/K and K/k algebraic, then F/k is also algebraic.

Hint: Choose any element and show its extension is finite over k.

Proof: Given any element $\alpha\in F$, α is algebraic over K so there exists an irreducible polynomial $a_nx^n+\cdots+a_0$, $a_i\in K$ to which α is a root. Moreover, K is algebraic over k so each a_i is algebraic over k. Thus in fact $k(a_0,\dots,a_n)$ is algebraic over k and $k(a_0,\dots,a_n,\alpha)$ is algebraic over $k(a_0,\dots,a_n)$. Notice $[k(a_0,\dots,a_n,\alpha):k(a_0,\dots,a_n)]=n$ as the irreducible polynomial has degree n, and $k(a_0,\dots,a_n)$ is a finite extension also of k as it is a finite number of simple extensions. Thus the degree $[k(a_0,\dots,a_n,\alpha),k]$ is finite and thus algebraic. Therefore α is algebraic over k. Since we began by selecting any $\alpha\in F$ it follows all of F is algebraic over k. □

5 Simple Extensions. – True or False? The extension $\mathbb{Q}(i,\sqrt{5})$ is simple.

Hint: Compare it to $\mathbb{Q}(i+\sqrt{5})$

Example: Consider $\mathbb{Q}(i+\sqrt{5})$. Notice $(i+\sqrt{5})^2=-1+2i\sqrt{5}+5=4+2i\sqrt{5}$, and so in fact $i\sqrt{5}$ is in the extension as $-4,1/2\in\mathbb{Q}$. Thus $1+i\sqrt{5}\in\mathbb{Q}(i+\sqrt{5})$. Now take

$$(i+\sqrt{5})(1+i\sqrt{5})=i+5i+\sqrt{5}-\sqrt{5}=6i.$$

As $1/6\in\mathbb{Q}$ it follows $i\in\mathbb{Q}(i+\sqrt{5})$ and so $-i$ is as well allowing us to conclude $\sqrt{5}\in\mathbb{Q}(i+\sqrt{5})$ so that $\mathbb{Q}(i,\sqrt{5})\le\mathbb{Q}(i+\sqrt{5})$ Since the reverse inequality is trivial we may actually assert $\mathbb{Q}(i,\sqrt{5})=\mathbb{Q}(i+\sqrt{5})$ so it is visibly a simple extensions. □

6 Irreducible Polynomials. Let p be prime. Then the polynomial $f(x)=1+x+\cdots+x^{p-1}$ in $\mathbb{Q}[x]$ is irreducible.

Hint: Use Eiseinstein's Criterion.

Proof: If $p=2$ then $f(x)=1+x$ which is irreducible as it is a monomial. Now let $p>2$.

This follows from a clever application of the Eisenstein Criterion. If we substitute $1+x$ for x in $f(x)$, (by the evaluation homomorphism) we shift all roots to the left by 1 – formally any root α of $f(x)$, yields the root $\alpha - 1$ of $f(1+x)$; thus if $f(1+x)$ is irreducible then so is $f(x)$, by the contrapositive of the statement.

$$f(1+x) = 1 + (1+x) + \cdots + (1+x)^{p-1} = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1}.$$

Recall

$$(1+x)^n = 1 + \binom{n}{1}x + \cdots + \binom{n}{k}x^k + \cdots + x^n$$

so that

$$a_i = \sum_{j=i}^{p-1} \binom{j}{i} = p\binom{p-1}{i}, \qquad i < p-1.$$

First $a_{p-1} = 1$. Also p divides each a_i, $0 \le i < p-1$ and $p^2 \nmid a_0 = p$. So by the Eisenstein criterion $f(x+1)$ is irreducible. $\square$

Hint: Consider the statement in terms of Galois groups.

7 Normal Transitivity. – True or False? If $F/K/k$ are field extensions with F/K and K/k normal, then F/k is also normal.

Example: Consider $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. As $\pm\sqrt[4]{2}$ is a root of $x^4 - 2$ with the other two roots being complex, we do not have all the roots of $x^4 - 2$ in $\mathbb{Q}(\sqrt[4]{2})$ proving the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal.

However at the same time notice that $\pm\sqrt{2}$ are the only roots of $x^2 - 2$ so $\mathbb{Q}(\sqrt{2})$ is a splitting field for $x^2 - 2$ so it is a normal extension over $\mathbb{Q}$. Also, $\pm\sqrt[4]{2}$ are the only roots of $x^2 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$, so indeed $\mathbb{Q}(\sqrt[4]{2})$ is a splitting field over $\mathbb{Q}(\sqrt{2})$ of $x^2 - \sqrt{2}$ and hence the extension is normal.

In the end we have a tower of normal extensions but the overall extension is not normal so we have disproved the transitivity of normality.[1] $\square$

Hint: Consider $\mathbb{Q}$ as fixed and that the squares of the square roots are distinct.

8 Field Isomorphisms. – True or False? $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic fields.

Example: First we construct the irreducible polynomials associated with the extensions. Certainly i is a root of the unique monic lowest degree irreducible polynomial $x^2 + 1$ in $\mathbb{Q}$. Likewise $x^2 + 2$ is the unique monic irreducible polynomial with root $\sqrt{2}$ – both so because we require even, positive, degree to reverse the squareroot function so no lower degree polynomial will suffice.

Now to conclude they are not isomorphic consider constructing a $\mathbb{Q}$-isomorphism. Let $\varphi = id_{\mathbb{Q}}$. From Thm-2.3.14 we know there exists a field isomorphism $\hat{\varphi} : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$ extending φ if and only if $\varphi(irr(i,\mathbb{Q})) = irr(\sqrt{2},\mathbb{Q})$. But notice a field isomorphism (indeed homomorphism) must send 1 to 1, so $\varphi(x^2+1) = x^2 + 1 \neq x^2 + 2$. Thus we cannot extends the isomorphism φ to be between $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$.

Well this does not preclude the existence of an isomorphism between $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ which is not a $\mathbb{Q}$-isomorphism. However if such an isomorphism φ exists then notice it too is required to map 1 to 1. This then forces $\varphi|_{\mathbb{Z}} = id_{\mathbb{Z}}$, as 1 generates $\mathbb{Z}$. Moreover this then requires

$$1 = \varphi(1) = \varphi(n \cdot 1/n) = \varphi(n)\varphi(1/n) = n\varphi(1/n),$$

so $1/n = \varphi(1/n)$. But then notice in fact

$$\varphi(a/b) = \varphi(a)\varphi(1/b) = a/b;$$

[1] Notice that a splitting field for $x^4 - 2$ has Galois group D_8 which is the first counter example for normal transitivity in groups.

thus, $\varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}$. Hence all isomorphism must be $\mathbb{Q}$-isomorphisms, but none such exist so there are in fact no isomorphisms between $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$. $\square$

9 Transcendental Extensions. If β is algebraic over $k(\alpha)$ and β is transcendental over k, then α is algebraic over $k(\beta)$.

Hint: Construct a new polynomial over $k(\beta)$ which annihilates α from a polynomial killing off β over $k(\alpha)$.

Proof: Given β is algebraic over $k(\alpha)$ it follows there exists some polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ in $k(\alpha)$ to which β is a root. Moreover, since β is transcendental over k, not all of the coefficients a_i are in k, or otherwise the polynomial would lie in $k[x]$ make β algebraic over k. Thus for some a_i, some positive power of α is exhibited. If we substitute all instances of α in $f(\beta)$ with y, and call this $f'(y)$, then $f'(y)$ is a polynomial in x for which $f'(\alpha) = f(\beta) = 0$; hence, α is a root of some polynomial of $k(\beta)$ proving α is algebraic over $k(\beta)$. $\square$

10 Domain Extensions. – True or False? If K/k is algebraic and D is an integral domain such that $k \leq D \leq K$, then D is a field.

Hint: Show $k(a) \leq D$ for any $a \in D$.

Proof: Take any $a \in D$. Since $a \in K$ it follows a is algebraic over k. Hence $k(a) = k[a, a^2, \ldots, a^n]$ is an algebraic extension. Notice $k(a)$ simply consists of all powers, sums, and products of elements in k and and of a, all of which are in D as well, so $k(a) \leq D$. However, $k(a)$ is a field so there exist an $a^{-1} \in k(a)$. But this requires then that $a^{-1} \in D$ so that D is closed to inverses. Thus in fact D is an integral domain. $\square$

11 Algebraic Extensions. Let K/k be a field extension. This extension is algebraic if and only if for every intermediate field F every k-monomorphic from F to F is in fact a k-automorphism of F.

Hint: Use the finiteness of an algebraic $k(a)$ extension for surjectivity. For the converse use the contrapositive.

Proof: Suppose K/k is algebraic and let F be an intermediate field. It follows for every $\alpha \in F$, that α is algebraic so that in fact $[k(\alpha) : k]$ is finite. Thus given any monomorphism $\varphi : F \to F$, it is clear $\varphi|_{k(\alpha)}$ is also a monomorphism, and as such it has a trivial kernel. Pick any basis $\{e_1, \ldots, e_n\}$ of $k(\alpha)$ over k and consider $\{f(e_1), \ldots, f(e_n)\}$. Take any $a_i \in k$, where

$$f(a_1e_1 + \cdots + a_ne_n) = a_1f(e_1) + \cdots + a_nf(e_n) = 0.$$

Since the kernel is trivial, it follows $a_1e_1 + \cdots a_ne_n = 0$ but as $\{e_1, \ldots, e_n\}$ is a basis we require $a_i = 0$ for all i; hence, $\{f(e_1), \ldots, f(e_n)\}$ is linearly independent. As $k(\alpha)$ over k has dimension n it follows this is in fact a basis, so $\varphi|_{k(\alpha)}$ is an automorphism of $k(\alpha)$ as it is now seen to be onto $k(\alpha)$.

Now suppose for some $\alpha \in F$ that $\alpha \notin \varphi(F)$. Then certainly $\varphi|_{k(\alpha)}$ is not an automorphism of $k(\alpha)$ which is a contradiction of our earlier work. Therefore φ is surjective and thus it is an automorphism of F.

For the converse consider the contrapositive. Let $\tau \in K$ be transcendental over k. As such we know $\{1, \tau, \tau^2, \ldots\}$ is a basis of the extension $k(\tau)/k$. So define a map $\varphi(\tau) = \tau^2$. This determines a unique homomorphism where $\{1, \tau, \tau^2, \ldots\}$ maps to $\{1, \tau^2, \tau^4, \tau^6, \ldots\}$. As this new set is still linearly independent it follows the map in injective, and, moreover, 1 maps to 1, so it is a k-monomorphism. Finally as τ is not in the image it is not an automorphism of $k(\tau)$. $\square$

12 Perfect Fields. A field F is called *perfect* if every irreducible polynomial over F is separable. Show that a field F of characteristic p is perfect if and only if every element of F has a p^{th} root in F. Show that every finite field is perfect.

Hint: Cite the canonical form for separable polynomials.

Proof: [Rot02, Prop. 6.79] Suppose F is a perfect characteristic p field. For every $a \in F$ there is a polynomial $x^p - a$. Since F is perfect, $x^p - a$ is separable, meaning it does not have multiple roots in a splitting field. However notice it carries the canonical form of an inseparable polynomial and is in a characteristic p field. Then to avoid a contradiction, $x^p - a$ must not satisfy the hypothesis of this result (Prop-2.6.18), that is, that $x^p - a$ must be reducible. Therefore there exists a p^{th} root of a in F.

Now suppose a field F has characteristic p and each element contains a p^{th} root in F. The only possible irreducible inseparable polynomials take the form:

$$f(x) = a_0 + a_1x^p + \cdots + a_nx^{pn}.$$

Since every element of F has a p^{th} root we may take each $a_i = b_i^p$ for some $b_i \in F$. Moreover, we may now express $f(x)$ as:

$$\begin{aligned} f(x) &= b_0^p + b_1^p x^p + \cdots + b_n^p x^{pn} \\ &= b_0^p + (b_1x)^p + \cdots + (b_nx^n)^p \\ &= (b_0 + b_1x + \cdots b_nx^n)^p. \end{aligned}$$

(As we are in a field of characteristic p, the Freshman's Dream applies for the last step.) Since $f(x)$ is visibly reducible, it follows all irreducible polynomials over F are separable, and so F is perfect.

Every finite field has prime characteristic, say p for a given field F. Notice that $x \mapsto x^p$ is field homomorphism when F has characteristic p (Freshman's Dream coupled with rules of exponents.) So it is a monomorphism, as $1 \mapsto 1$, and furthermore by the pigeon-hole-principle it follows it is surjective; therefore it is an isomorphism which simply means $F = F^p$ and every element has a p^{th} root, so F is perfect. $\square$

Hint: Consider the roots forming a basis of the extension.

13 Transitive Actions on Roots. Let $f \in k[x]$, K/k be a splitting field for f over k, and $G = Gal(K/k)$. Show that G acts on the set of roots of f. Show that G acts transitively if f is irreducible. Conversely, if f has no multiple roots and G acts transitively then f is irreducible.

Proof: Take $\sigma, \tau \in G$. Since f splits in K it follows there are $\alpha, \alpha_i \in K$ such that

$$f(x) = \alpha(x - \alpha_1)\cdots(x - \alpha_n),$$

and also that $K = k(\alpha_1, \dots, \alpha_n)$. Since each automorphism of G is a function, the action of G on $\{\alpha_1, \dots, \alpha_n\}$ defined as $\sigma \cdot \alpha_i = \sigma(\alpha_i)$ is well-defined. Notice $\sigma(\tau(\alpha_i)) = (\sigma\tau)(\alpha_i)$, by the fact that multiplication in G is composition. Also the identity map leaves all elements invariant; thus, G does indeed act on $\{\alpha_1, \dots, \alpha_n\}$.

When f is irreducible, all the roots of f are outside k. As K is a splitting field, it follows it is normal and finite. Thus applying Prop-2.7.8, it follows there exists an element $\sigma \in G$, for each (i, j), such that $\sigma(a_i) = a_j$. That is to say that G acts transitively.

Finally, if f has no multiple roots and G acts transitively, K remains a splitting field of f so K/k is still normal and finite; moreover, with no multiple roots it is a separable extension. Now applying Coro-2.7.15 we may assert G has the order n. Since G acts transitively on n elements, it follows every non-trivial element acts non-trivially on K. If any root α_i actually lies in k, then G must act trivially on this element – for G is the set of all k-automorphisms of K. To avoid this contradiction we require each α_i be outside k; thus, f is irreducible as it has no root in k. $\square$

cases: charac-

14 Infinite Field Multiplication. Prove that if F is an infinite field, then its multiplicative group $F^\times$ is never cyclic.

Proof: If F has characteristic 0, then $\mathbb{Q}$ is embedded in F, and so $\mathbb{Q}^\times$ lies in $F^\times$. Notice 2 and 3 are relatively prime, so $\mathbb{Q}^\times$ is not cyclic, and hence neither is $F^\times$.

Suppose F has characteristic p; then the prime subfield is isomorphic to $\mathbb{Z}_p$. If $F^\times$ is to be cyclic, it most certainly is infinite, so it is isomorphic to $\mathbb{Z}$. However, $\mathbb{Z}$ is torsion free and $\mathbb{Z}_p^\times$ is nothing but torsion. $F^\times$ is acyclic. □

15 Partial Splits. Let K/k be a normal field extension and f be an irreducible polynomial over k. Show that all irreducible factors of f in $K[x]$ all have the same degree.

Hint: PENDING:

Proof: Since $f(x)$ is irreducible over k, it follows $f(x) = a(b(x))$ for some $a(x), b(x) \in k[x]$ where $a(x)$ is irreducible over k (or else $f(x)$ would not be) and has a root in K – otherwise it would have no proper factors in K either. However, K/k is normal, so $a(x)$ has all its roots in K so it splits in K as follows:

$$a(x) = \alpha(x - \alpha_1)\cdots(x - \alpha_m).$$

Consequently

$$f(x) = \alpha(b(x) - \alpha_1)\cdots(b(x) - \alpha_m).$$

Suppose $b(x) - \alpha_1$ is reducible. Consider the k-automorphism σ sending α_1 to α_j. We know σ exists because both α_1 and α_j are roots of the same irreducible polynomial, and furthermore we know the automorphism is closed to K because K is normal, thus containing all roots of $a(x)$. So clearly then any factorization of $b(x) - \alpha_1$ maps to an equivalent factorization of $b(x) - \alpha_j$ by σ; thus each component is irreducible if even one is irreducible.

Finally we simply take $a(x)$ to have the highest possible degree and since this requires each $b(x)$ to have the smallest possible degree not all can have factors. Since one $b(x) - \alpha_i$ is irreducible, so are they all, and hence every irreducible factor of $f(x)$ over $K[x]$ has the same degree – that of $b(x)$. □

16 Transcendental Galois Groups. – True or False? $Gal(k(x)/k) = \mathbf{1}$.

Hint: Consider substituting x with $1/x$.

Example: False. Indeed $Gal(k(x)/k) \cong GL_2(k)$. While the isomorphism is not important we can show that at least all of $GL_2(k)$ is contained in the Galois group.

Consider the map

$$\Gamma(p(x)) = p\left(\frac{ax+b}{cx+d}\right), \qquad ad - bc \neq 0,$$

where $p(x)$ is any rational function in $k(x)$. If $a_0 \in k$ then $p(x) = a_0$ for any entry of x so indeed $\Gamma(p(x)) = a_0 = p(x)$ proving Γ is a k-fixing map. That Γ is well-defined follows because it is a an evaluation map.[2]

[2] Formally it is a substitution homomorphism so nothing but bijectivity need be checked. However as the map does not end in k, as we are substituting functions, it seem prudent to verify all steps for completeness.

Next we verify the homomorphism properties:

$$\begin{aligned}
\Gamma(p(x)+q(x)) &= \Gamma\left(\sum_{i=0}^{n}(p_i+q_i)x^i\right) \\
&= \sum_{i=0}^{n}(p_i+q_i)\left(\frac{ax+b}{cx+d}\right)^i \\
&= \sum_{i=0}^{n}p_i\left(\frac{ax+b}{cx+d}\right)^i + q_i\left(\frac{ax+b}{cx+d}\right)^i \\
&= p\left(\frac{ax+b}{cx+d}\right) + q\left(\frac{ax+b}{cx+d}\right) \\
&= \Gamma(p(x)) + \Gamma(q(x)).
\end{aligned}$$

Now for multiplication:

$$\begin{aligned}
\Gamma(p(x)q(x)) &= \Gamma\left(\sum_{i=0}^{n}\sum_{j=0}^{m}p_iq_jx^{i+j}\right) \\
&= \sum_{i=0}^{n}\sum_{j=0}^{m}p_iq_j\left(\frac{ax+b}{cx+d}\right)^{i+j} \\
&= \sum_{i=0}^{n}\sum_{j=0}^{m}p_i\left(\frac{ax+b}{cx+d}\right)^{i}q_j\left(\frac{ax+b}{cx+d}\right)^{j} \\
&= \sum_{i=0}^{n}p_i\left(\frac{ax+b}{cx+d}\right)^{i}\sum_{j=0}^{m}q_i\left(\frac{ax+b}{cx+d}\right)^{j} \\
&= \Gamma(p(x))\Gamma(q(x)).
\end{aligned}$$

Finally we realize that

$$\Gamma\left(\frac{p(x)}{q(x)}\right) = \frac{\Gamma(p(x))}{\Gamma(q(x))}$$

so indeed it is sufficient to test homomorphism only on polynomials; therefore, Γ is a k-homomorphism from $k(x)$ to $k(x)$ and as such must be a monomorphism as well.

Finally that Γ is invertible follows from the assumption that $ad \neq bc$. This makes the matrix invertible so that we have:

$$\Gamma^{-1}(p(x)) = p\left(\frac{-dx+b}{cx-a}\right).$$

Clearly then

$$\Gamma(\Gamma^{-1}(p(x))) = p\left(\frac{a\frac{-dx+b}{cx-a}+b}{c\frac{-dx+b}{cx-a}+d}\right) = p(x)$$

and likewise:

$$\Gamma^{-1}(\Gamma(p(x))) = p\left(\frac{-d\frac{ax+b}{cx+d}+b}{c\frac{ax+b}{cx+d}-a}\right) = p(x).$$

So Γ is $k(x)$ automorphism fixing k. Hence $\Gamma \in Gal(k(x)/k)$. Moreover there is a canonical bijection between Γ and the matrix

$$A(\Gamma) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad det(A(\Gamma)) \neq 0$$

so indeed we have an embedding of $GL_2(k)$ in $Gal(k(x)/k)$ so the Galois group is not trivial. $\square$

17 Field Extensions. Construct subfields of $\mathbb{C}$ which are splitting fields over $\mathbb{Q}$ for polynomials $x^3 - 1$, $x^4 - 5x^2 + 6$, and $x^6 - 8$. Find the degrees of those fields as extensions over $\mathbb{Q}$.

Hint: Adjoin any real roots first, then find the appropriate primitive complex roots.

Example:

- The third roots of unity are 1,

  $$\omega = e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}; \qquad \omega^2 = e^{4\pi i/3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

  For our extension we may drop the rational translations and coefficients to obtain $\mathbb{Q}(i\sqrt{3})$ as a splitting field of $x^3 - 1$. In particular by dividing by $x - 1$ we find $x^2 + x + 1$ is the irreducible component of $x^3 - 1$ and so the degree of the extension is 2.

- We begin by factoring our polynomial in $\mathbb{C}$:

  $$x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x + \sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2}).$$

  Thus the extension $\mathbb{Q}(\sqrt{2}, i)$ is our desired splitting field. This gives us a basis for our splitting field of

  $$\{1, \sqrt{2}, i, i\sqrt{2}\}.$$

  Therefore the degree of the extension is 4.

- When considering $x^6 - 8$, we begin by considering the sixth roots of unity, which are:

  $$\left\{\pm 1, \left(\pm\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right)\right\}$$

  and the radius is $\sqrt[6]{8} = \sqrt{2}$, so our splitting field is $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$. As

  $$x^2 - 2 = irr(\sqrt{2}; \mathbb{Q}) \neq irr(i\sqrt{3}; \mathbb{Q}) = x^3 + 3$$

  it follows

  $$\{1, \sqrt{2}, i\sqrt{3}, i\sqrt{6}\}$$

  is a basis for the extension, and thus it has degree 4.

$\square$

18 Normal Extensions. Which of the following extensions are normal?

Hint: Try to verify if they are splitting fields for some polynomial.

(a) $\mathbb{Q}(x)/\mathbb{Q}$;

(b) $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$;

(c) $\mathbb{Q}(\sqrt[7]{5})/\mathbb{Q}$;

(d) $\mathbb{Q}(\sqrt{5}, \sqrt[7]{5})/\mathbb{Q}(\sqrt[7]{5})$;

(e) $\mathbb{R}(\sqrt{-7})/\mathbb{R}$.

Example:

(a) Let $p(x)$ be an irreducible polynomial over $\mathbb{Q}$. Then $p(x)$ has all its roots in $\mathbb{C}$, but $\mathbb{C} \cap \mathbb{Q}(x) = \mathbb{Q}$ so $\mathbb{Q}(x)$ has no roots of $p(x)$, and thus vacuously $\mathbb{Q}(x)/\mathbb{Q}$ is normal. (Also recall its Galois group was trivial so normality it for free.)

(b) The polynomial $x^2 + 5$ has $\pm i\sqrt{5}$ as a roots. It is enough now to claim $\mathbb{Q}(i\sqrt{5})/\mathbb{Q}$ is the splitting field of an irreducible polynomial so it is a normal extension.

(c) Here note that $x^7 - 5$ is irreducible by the rational roots theorem. Moreover it has as a root, $\sqrt[7]{5}$. However it does not contain

$$\omega = \sqrt[7]{5}(e^{i\frac{2\pi}{7}}),$$

as $\mathbb{Q}(\sqrt[7]{5}) \subseteq \mathbb{R}$ and $\omega \notin \mathbb{R}$ since $sin(\frac{2\pi}{7}) \neq 0$. Therefore we have an irreducible polynomial with one root in the extension but yet does not split; hence, the extension is not normal.

(d) Take $x^2 - 5$; the roots are $\pm\sqrt{5}$. Clearly any extension that contains one contains the other. Therefore any extension that is generated by one is a splitting field for $x^2 - 5$, and hence it is a normal extension.

(e) The polynomial $x^2 + 7$ has the roots $\pm i\sqrt{7}$ which again means the extension is normal if it is the extension of one of these. Hence $\mathbb{R}(i\sqrt{7})/\mathbb{R}$ is normal. In both these last two cases, the fact that the extension is of index 2 explains why the extension is normal.

□

Hint:

19 Extension Degrees. Let K/k be a splitting field for a polynomial $f(x) \in k[x]$ of degree n. Show that $[K : k]$ divides $n!$.

Proof: The case for inseparable polynomials is unclear. We pretend these are not important.

We know $[K : k] = |Gal(K/k)|$. Moreover, from our previous exercises we know that the automorphisms in $Gal(K/k)$ are uniquely determined by the permutations they make on the roots of the irreducible polynomials that generate the extension. Since K/k is splitting field for $f(x)$, it follows the roots $a_1, \dots, a_n$ of $f(x)$ determine $K \cong k(a_1, \dots, a_n)$. At best $f(x)$ is irreducible at which point the automorphisms may permute the n roots in what ever fashion they wish; hence, $Gal(K/k) = S_n$, so $[K : k] = n!$. But if $f(x)$ is reducible, then the automorphisms must only permute the roots within the irreducible factors in which they are found. Therefore $Gal(K/k)$ is a subgroup of S_n and so by the theorem of Lagrange $[K : k] = Gal(K/k)|n!$. □

Hint: Consider a transcendental extension.

20 Field Monomorphisms. – True or False? If K/k is a field extension then every k-monomorphism $K \to K$ is an automorphism.

Example: False. Consider the extension $k(x)/k$. If we define a map on the basis elements $1, x, x^2, \dots$ by sending 1 to 1, x to x^2, x^2 to x^4, and in general x^m to x^{2m}, we determine conclusively a linear mapping $f : k[x] \to k[x]$ which leaves k invariant. Moreover,

$$f(a(x)b(x)) = f(c(x)) = c(x^2) = a(x^2)b(x^2).$$

Now if we rationalize $k[x]$ we must ensure that $f' : k(x) \to k(x)$ remains well-defined, and we will thus have an monomorphism $k(x) \to k(x)$ which fixes k (recall fields have no ideals so the map is trivially monic.)

We define $f'(a(x)/b(x)) = f(a(x))/f(b(x))$. As $b(x) \neq 0$, it follows there exists a coefficient b_i of $b(x)$ which is non-zero. This element maps to b_{2i}, thus $f(b(x)) \neq 0$. Furthermore, given $a(x)/b(x) = c(x)/d(x)$, it is equivalent to state $a(x)d(x) = b(x)c(x)$. Notice:

$$a(x^2)d(x^2) = f(a(x)d(x)) = f(b(x)c(x)) = b(x^2)c(x^2);$$

thus, $f'(a(x)/b(x)) = f(c(x)/d(x))$ so f' is well-defined, and thus a k-homomorphism of $k(x)$ to $k(x)$.

Finally, notice that $f(k[x]) = k[x^2]$ so indeed $f'(k(x)) = k(x^2)$ which is a proper subset of $k(x)$, and hence f' is not surjective so it is not an automorphism. $\square$

21 Galois Groups. Determine the Galois groups fo the following extensions:

Hint: Determine the degrees of the extensions first.

(a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$;

(b) $\mathbb{Q}(\sqrt[5]{3}, e^{2\pi i/5})/\mathbb{Q}$;

(c) $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})/\mathbb{Q}$;

(d) $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}$.

(a) $G = Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = C_2 \times C_2$.

Example: The polynomials $x^2 - 2$ and $x^2 - 3$ are monic minimal irreducible polynomials for the roots $\sqrt{2}$ and $\sqrt{3}$ respectively. Hence the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has degree 2 as does its Galois group since we have a separable normal extension. Moreover, $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ so the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$ has degree 2 as well so by the tower law we have $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4 = |G|$.

Any automorphism in the Galois group may permute $\sqrt{2}$ with $-\sqrt{2}$ and likewise the pair $\pm\sqrt{3}$. Thus we recognize every permutation has at most order 2, so the group must be $C_2 \times C_2$. $\square$

(b) $G = Gal(\mathbb{Q}(\sqrt[5]{3}, e^{2\pi i/5})/\mathbb{Q}) = Mr_{20}$.

$$Mr_{20} = \langle a, b \mid a^5 = b^4 = 1, bab^{-1} = a^2 \rangle.$$

Example: Since 5 is prime, $e^{2\pi i/5}$ is a primitive 5th root of unity. Moreover, $\sqrt[5]{3}$ is a root of $x^5 - 3$ so the extension is a splitting field for $x^5 - 3$. There is only one real root as the derivative is nowhere negative so the graph is increasing, thus having only one x-intercept. Therefore

$$p(x) = \frac{x^5 - 3}{x - \sqrt[5]{3}}$$

is irreducible over $\mathbb{R}$ and so also over $\mathbb{Q}(\sqrt[5]{3})$. Clearly $p(x)$ has degree 4 so we have finally that

$$[\mathbb{Q}(\sqrt[5]{3}, e^{2\pi i/5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{3}, e^{2\pi i/5}) : \mathbb{Q}(\sqrt[5]{3})][\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 20.$$

Since $p(x)$ is not over $\mathbb{Q}$ it follows the roots are acted upon transitively. Therefore we need a transitive subgroup of S_5 of order 20. S_5 cannot have an element of order 10 – requires $(12345)(67)$ cycle or greater.

Let G be a group of order 20. By the third Sylow theorem we know there exists a unique Sylow 5-subgroup, which must be isomorphic to C_5. Let S_4 be a Sylow 2-subgroup, it must have order 4. As $(5,4) = 1$ it follows C_5 and S_4 intersect trivially. Moreover, $C_5 S_4 = G$ by the pigeon-hole-principle. As C_5 is the unique Sylow 5-subgroup it is normal in G. If we can establish that $G/C_5 \cong S_4$ we will be able to assert that $G = C_5 \rtimes S_4$.

Suppose $S_4 = C_4$. Then there is precisely one C_2 subgroup of S_4 which intersects C_5 trivially, so it produces an order 10 subgroup $C_5 < C_5C_2 < G$. Moreover, if $C_5C_2 \cong C_{10}$, then any other Sylow 2-subgroup must intersect C_5C_2 as there are only 10 elements left and if there is more than one C_4 subgroup, these elements must all be their generators; thus their C_2 subgroups are all the same. Finally if $C_5C_2 \cong D_5$ – the only other possibility, then again as D_5 require 5 involutions, all the C_2 subgroups of the C_4's intersect C_5C_2. Therefore, the only intermediate subgroup between C_5 and G is C_5C_2 so $G/C_5 \cong C_4$ whenever $S_4 \cong C_4$.

Suppose $S_4 = C_2 \times C_2$. Here the argument in simpler. If C_5C_2 contains any two non-trivial elements of S_4 then it contains all of S_4 so it generates G. This cannot be as we know C_5 is normal so C_5C_2, which has order 10, is a proper subgroup. Therefore each of the three proper subgroups of S_4 generate their own order 10 subgroup, so in fact G/C_5 has three proper subgroups so it must be $C_2 \times C_2$.

Now we can sum up our result with the claim that the following diagram is split exact:

$$\mathbf{1} \longrightarrow C_5 \hookrightarrow G \twoheadrightarrow S_4 \longrightarrow \mathbf{1}.$$

Whence, there exists a homomorphism $\varphi : S_4 \to Aut\ C_5 = C_4$. This determines the following table: (let $\langle a \rangle = C_5$ and $b \in S_4$)

$$\varphi : C_4 \twoheadrightarrow C_4;$$

$$\varphi : C_4 \twoheadrightarrow C_2 \hookrightarrow C_4;$$

$$\varphi : C_4 \twoheadrightarrow \mathbf{1} \hookrightarrow C_4;$$

$$\varphi : C_2 \times C_2 \twoheadrightarrow C_2 \hookrightarrow C_4;$$

$$\varphi : C_2 \times C_2 \twoheadrightarrow \mathbf{1} \hookrightarrow C_4.$$

Which produces the following corresponding groups:[3]

$$\begin{aligned}
Mr_{20} &= \langle a, b \mid a^5 = b^4 = 1, bab^{-1} = a^2 \rangle \\
Q_{20} &= \langle a, b \mid a^5 = b^4 = 1, bab^{-1} = a^{-1} \rangle \\
\mathbb{Z}_{20} &= \langle a, b \mid a^5 = b^4 = 1, bab^{-1} = a \rangle \\
D_{20} &= \langle a, b \mid a^5 = b^2 = 1, bab^{-1} = a^{-1} \rangle \\
\mathbb{C}_2 \times C_{10} &= \langle a, b \mid a^5 = b^2 = 1, bab^{-1} = a \rangle
\end{aligned}$$

[3] The presentations all have the order of a and b together with a normal form relation; thus they determine at most 20 elements, and by their construction at least 20, so they are necessary and sufficient.

We can observe that all but Mr_{20} have $\mathbb{Z}_{10}$ as a subgroup. However we know our Galois group lies in S_5 so as there is no element of order 10 in S_5 we must conclude the Galois group is Mr_{20}.[4] □

(c) $G = Gal(\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})/\mathbb{Q}) = C_2$

Example: Notice the irreducible polynomial $x^2 - 2$ splits in our extension but the polynomial $x^3 - 2$ only does so partially. Hence our given extension is not normal. As such we only have the roots $\pm\sqrt{2}$ and $\sqrt[3]{2}$ to permute, but we cannot mix roots of different irreducible factors. Hence we only have permutations that transposed $pm\sqrt{2}$, so the Galois group is C_2. □

(d) $G = Gal(\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}, e^{2\pi i/3})/\mathbb{Q}) = C_2 \times S_3$

Example: Since $irr(\sqrt{2}; \mathbb{Q}) = x^2 - 2$ and $irr(\sqrt[3]{2}; \mathbb{Q}(\sqrt{2})) = x^3 - 2$ (irreducibility follows from rational roots theorem) it follows our extension is simply

$$\mathbb{Q}(\sqrt{2}, \sqrt[2]{2}, \omega)/\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$$

where we let $\omega = e^{2\pi i/3}$ which is a primitive third root of unity.

As such from the tower law we see the degrees of the extension are determined by the irreducibles that cause them: so $deg\ x^2 - 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$, $deg\ x^3 - 2 = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})]$, and finally $deg\ x^2 + x + 1 = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})]$ so our total extension degree is 12.

As this is the splitting field for $(x^2 - 2)(x^3 - 2)$ we see that it is normal and separable so its Galois group has order 12.

Since we have the intermediate field $\mathbb{Q}(\sqrt{2})$ of degree 2 it is normal, so $H = Gal(\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt{2})) \lhd G$, and moreover H has order 6. Also, (ω, ω^2) is a permutation required by the transitive action on the roots of $x^2 + x + 1$ and it fixed $\sqrt{2}$ so $(\omega, \omega^2) \in H$. Also, the roots of $x^3 - 2$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ and are acted upon transitively so there must be a 3-cycle $\sigma = (\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ in G. But as this fixes $\sqrt{2}$ it is clear $\sigma \in H$ also. Hence visibly H is non-abelian so $H \cong S_3$. Finally we can rearrange the tower to have an intermediate field $\mathbb{Q}(\sqrt[3]{2}, \omega)$ which has degree 6 over $\mathbb{Q}$ as it is the splitting field for $x^2 - 3$, and it also normal for the same reason. Thus we have an order 2 subgroup K of G which does not intersect H and that meets H at G, so we have the conditions for an internal direct product. Hence from the isomorphism types of H and K we know $G \cong C_2 \times S_3$. □

22 Finite Fields. Prove that the quotient ring $R := \mathbb{F}_3[x]/(x^2 + 1)$ is a field of order 9. Exhibit an explicit generator for $R^\times$.

Hint: Find the dimension of the field as an $\mathbb{F}_3$ vector space.

Example: Notice $x^2 + 1$ is irreducible in $\mathbb{F}_3$ since

$$0^2 \equiv 0, \qquad 1^1, 2^2 \equiv 1 \pmod 3.$$

As such, $x^2 + 1$ is the monic irreducible polynomial of its roots, and R is thus an extension containing one of its roots i. Notice the degree of the extension is 2 as the polynomial has degree 2. Hence, $R = \mathbb{F}_3(i)$ and $\{1, i\}$ is a basis for $R/\mathbb{F}_3$. Visibly then $R = \mathbb{F}_3 \oplus \mathbb{F}_3$ as a vector space, and so it has order 9.

[4] The title of Mr. 20 is clearly not a standard name for this group.

Finally, the element $1+i$ generates $R^\times$ as

$$(1+i)^2 \equiv 2i, \qquad (1+i)^4 \equiv (2i)^2 \equiv 2, \qquad (1+i)^8 \equiv 2^2 \equiv 1 \pmod 3.$$

Hence $(1+i)$ has order at least 8, in a group of degree 8, so it is a cyclic generator. $\square$

Hint: Show the Frobenius homomorphism is injective.

23 p^k-th roots in Finite Fields. – True or False? If F is a field of characteristic p, $\alpha \in F$, then F contains at most one p^kth root of α.

Proof: True. We must show that $x^{p^k} = y^{p^k}$ implies $x = y$ for all $x, y \in F$. This will not ensure the existence of p^kth roots, but it will determine them to be unique upon existence. Notice this is a short application of the Freshman's Dream:

$$0 = (x^{p^k} - y^{p^k}) = (x-y)^{p^k}.$$

This implies $(x-y)(x-y)^{p^k-1} = 0$, so $x - y$ is a zero-divisor. In a field this requires $x - y = 0$, and so $x = y$. $\square$

Hint: All such extensions are algebraic.

24 Normal Extensions of $\mathbb{C}$. – True or False? Every finite normal extension of $\mathbb{C}$ is normal over $\mathbb{R}$.

Proof: True. Every finite extension of $\mathbb{C}$ is an algebraic extension. Yet $\mathbb{C}$ is algebraically closed, so there are no polynomials with roots outside it, and so every finite extension is a trivial extension. Thus every finite extension is $\mathbb{C}/\mathbb{C}$ and so as $\mathbb{C}/\mathbb{R}$ is normal, so is every finite extension of $\mathbb{C}$. $\square$

Hint: Construct a polynomial that annihilates the given rational function.

25 Rational Function Fields. Let F be a field, and $F(x)$ be the field of rational functions. Show $F(x)/F(\frac{x^3}{x+1})$ is a simple extension, determine its degree, and $irr(x; F(\frac{x^3}{x+1}))$.

Example: To construct a polynomial over $F(\frac{x^3}{x+1})$ with x as a root, we need to ride ourselves of the fraction. Since x is to be our root we will consider inverting our fraction as $\frac{x+1}{x^3}$. Here then we require the term $\frac{x+1}{x^3}y$ in our polynomial $p(y)$ in $F(\frac{x^3}{x+1})[y]$. Since we want the minimal degree we will look no further and use what we have to determine the remaining terms of the polynomial as:

$$p(y) = \frac{x+1}{x^3}y^3 - y - 1.$$

Since we want a monic minimal degree polynomial we will replace the polynomial with

$$p(y) = y^3 - \frac{x^3}{x+1}y - \frac{x^3}{x+1}.$$

By our construction this is monic and of minimal degree having x as a root, so since x is not in $F(\frac{x^3}{x+1})$ it is irreducible, and indeed $p(y) = irr(x; F(\frac{x^3}{x+1}))$. Hence, the extension is of degree 3, and as it is finite it is simple. $\square$

Hint: Consider division by any factor.

26 Normal Extensions. – True or False? If $[K:k] = 2$ then K/k is normal.

Proof: True. Suppose $[K:k] = 2$. Then there is a basis $\{1, a\}$ for the extension, and so visibly $a^2 \in k$. Thus $x^2 - a^2$ is an irreducible polynomial in $k[x]$ which splits in K, so the extension is normal. $\square$

Hint: Follow a root through irreducible decompositions of an irreducible over k, K, and finally F.

27 Separable Transitivity. For extensions $F/K/k$, if F/K and K/k are separable then F/k is separable.

Proof: Take an irreducible polynomial $p(x)$ in $k[x]$. Over $K[x]$ $p(x)$ factors into irreducible components. Since the extension K/k is separable no irreducible component appears more than once, and thus each root appears in exactly one of the irreducible components.

Now take any irreducible component and move to $F[x]$. Here the polynomial may factor further into irreducible components. However, as F/K is separable, once again each root appears exactly once and in exactly one of these second generation irreducible components. Therefore together we see that every root is a simple root over F. So F/k is separable. $\square$

28 Counting Polynomials. Let p be prime. Then there are exactly $(q^p - q)/p$ monic irreducible polynomials of degree p in $\mathbb{F}_q[x]$.

Hint: Count the number of roots for each irreducible.

Proof: For every irreducible polynomial of degree p, the splitting field is $\mathbb{F}_{q^p}$ as there is only one finite field of this order. Now the extension is a splitting field so it is normal. Since p is prime there are no intermediate fields either. Now every element α in $\mathbb{F}_{q^p} \backslash \mathbb{F}_q$ is irreducible and algebraic over $\mathbb{F}_q$ as the extension is finite. With no intermediate fields it follows the $irr(\alpha; \mathbb{F}_q)$ has degree p. Therefore of the $q^p - q$ elements, each corresponds to an irreducible polynomial of degree p. Since all finite field extensions are separable, each $irr(\alpha; \mathbb{F}_q)$ actually absorbs p many elements so we have a total of $\frac{q^p-q}{p}$ irreducible polynomials over $\mathbb{F}_q$. $\square$

29 Intermediate Finite Fields. Let $q = p^n$ and $d|n$. Then $\mathbb{F}_q$ contains exactly one subfield with p^d elements. Conversely, if $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$ then $d|n$.

Hint: The Galois group of a finite field is cyclic.

Proof: We know the Galois group of a finite field extension over a finite field is cyclic. Moreover, if the degree of the extension is n, then the Galois group has order n so it is the cyclic group C_n. Therefore from the Galois correspondence we know there is one and only one subfield of degree d over the prime subfield, for every $d|n$. $\square$

30 Splitting Fields. If K/k is a finite normal separable field extension, then there exists an irreducible polynomial $f \in k[x]$ such that K is a splitting field for f over k.

Hint: Notice the extension is simple.

Proof: Since the extension is finite and separable we know it is a simple extension. Thus $K = k(\alpha)$ for some α. Since the extension is finite it is algebraic so $irr(\alpha; k)$ has a root in K. Yet K is normal so it follows all the roots of $irr(\alpha; k)$ are in K so indeed $irr(\alpha; k)$ splits in K. And moreover K is a splitting field of $irr(\alpha; k)$. $\square$

31 Simple Extensions. Every finite field extension is simple.

Hint: Consider an inseparable extension.

Example: Consider $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$. Since it is the tower of extensions $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y)/\mathbb{F}_p(x^p, y^p)$ we see the degree is p^2 – as there minimal monic irreducible polynomials are $z^p - x^p$ and $z^p - y^p$ respectively. However the extension is not simple. We notice that for every $a(x, y) \in F[x, y]$, we may use the Freshman's dream to get:

$$a(x, y)^p = \left(\sum_{i,j=0}^{m,n} a_{i,j} x^i y^j \right)^p = \sum_{i,j=0}^{m,n} a_{i,j}^p x^{ip} y^{jp} \in \mathbb{F}_p(x^p, y^p).$$

So rational functions $\frac{a(x)}{b(x)}^p$ are also in $\mathbb{F}_p(x^p, y^p)$. Hence no element in $\mathbb{F}_p(x, y)$

can have degree p^2 over $\mathbb{F}_p(x^p, y^p)$ so the extension is not simple. $\square$

Hint: Consider the Galois group of $\sqrt{a}, \sqrt{b}$.

32 Squares in Finite Fields. If F is a finite field and $a, b \in F$ are not squares then ab is a square.

Proof: Suppose all three are not squares in F. Then the extension $F(\sqrt{a}, \sqrt{b})$ (where $\sqrt{a}$ is a solution of $x^2 - a$) contains $\sqrt{ab}$ so it contains the three extensions

$$\begin{tikzcd}
 & F(\sqrt{a}, \sqrt{b}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
F(\sqrt{a}) \arrow[dr, dash] & F(\sqrt{ab}) \arrow[d, dash] & F(\sqrt{b}) \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

Now this may not be as the extension are all of degree 2 so it illustrates the Galois extension of $C_2 \times C_2$. Since It is also to be a finite extension of a finite field, it must have a cyclic Galois group. Therefore $\sqrt{a} = \sqrt{b}$ at which point aa is clearly a square. $\square$

Hint:

33 Simple Transitivity. Let $F/K/k$ with K/k finite separable and F/K simple. Then F/k is simple.

Proof: Since K/k is finite and separable it is indeed a simple extensions. So let $K = k(\alpha)$ for some $\alpha \in K$. Moreover, as the extension is finite, α is algebraic over k so $\alpha^n \in k$ for some k. Now as F/K is simple let $F = K(t)$. It follows $k(\tau + \alpha) \leq k(t, \alpha) = F$. We wish to show $F = k(t + \alpha)$ so that we may conclude the extension is simple. So consider

$$(u + \alpha)^n = \sum_{i=0}^{n} \binom{n}{i} u^{n-i} \alpha^i = \sum_{i=0}^{n-1} \binom{n}{i} u^{n-i} \alpha^i + \alpha^n.$$

Since $\alpha^n \in k$ it follows we have

$$u \left(\sum_{i=0}^{n-1} \binom{n}{i} u^{n-i} \alpha^i \right) \alpha \in k(\tau + \alpha).$$

$\square$

34

35 There is no irreducible polynomial of degree 4 over $\mathbb{Q}$ with splitting field of degree 6.

Proof: Since $\mathbb{Q}$ has characteristic 0, all irreducible polynomials are separable; thus, so is our degree 4 polynomial $p(x)$. Moreover, the splitting field will be a normal extension and also finite, so we have a Galois extension allowing us to conclude $|Gal(p; \mathbb{Q})| = 6$. As the Galois group acts transitively on the roots of our polynomial we have to find a transitive order 6 subgroup of S_4. But the best part is there are none (the only order 6 subgroups of S_4 are S_3^i, where i is a fixed point $1, \ldots, 4$.) So $p(x)$ does not exist. $\square$

37 Let φ be the Euler function and $\varepsilon \in \mathbb{C}$ be a primitive mth root of unity. Prove that $[\mathbb{Q}(\varepsilon + \varepsilon^{-1}) : \mathbb{Q}] = \varphi(m)/2$.

Proof: First of all note that the Euler-φ function is even for $m > 2$. When $m = 2$, the primitive 2th roots of unity is -1 which is in $\mathbb{Q}$ so the extension has degree 1. Now consider $m > 2$.

Now notice $x^2 + (\varepsilon + \varepsilon^{-1})x - 1$ is irreducible over $\mathbb{Q}(\varepsilon + \varepsilon^{-1})$ as it has as a root ε. Therefore $[\mathbb{Q}(\varepsilon) : \mathbb{Q}(\varepsilon + \varepsilon^{-1})] = 2$ so by the tower law $[\mathbb{Q}(\varepsilon + \varepsilon^{-1}) : \mathbb{Q}] = \varphi(m)/2$.

It is interesting to furthermore note the irreducible polynomial for the extension $\mathbb{Q}(\varepsilon + \varepsilon^{-1})/\mathbb{Q}$ is simply:

$$\Upsilon_m(x) = \prod_{a \leq m/2, (a,m)=1} (x - (e^{2\pi i \frac{a}{m}} + e^{2\pi i \frac{m-a}{m}}) = \prod_{a \leq m/2, (a,m)=1} \left(x - 2\cos\frac{2\pi a}{m} \right).$$

And in fact $\Upsilon_m(x) \in \mathbb{Z}[x]$. $\square$

38 Let $m > 1$ be an odd integer. Show that $\Phi_{2m}(x) = \Phi_m(-x)$.

Proof: Since m is odd, it follows $\varphi(m)$ is even, and $\varphi(2m) = \varphi(m)$.

$$\Phi_m(-x) = \prod_{i=1}^{\varphi}(m)(-x - \varepsilon_i) = (-1)^{\varphi}(m) \prod_{i=1}^{\varphi}(m)(x + \varepsilon_i) = \prod_{i=1}^{\varphi}(2m)(x - (-\varepsilon)).$$

Notice $(-\varepsilon_i)^{2m} - 1 = 0$ for all primitive mth roots of unity. Since m is odd, $(-\varepsilon)^d - 1 \neq 0$ for any $d|m$. Therefore recalling $x^{2m} - 1 = \prod_{d|2m} \Phi_d(x)$ we now see $-\varepsilon_i$ are the roots of Φ_{2m}; wherefore, $\Phi_m(-x) = \Phi_{2m}(x)$. $\square$

40 Show there exist $f \in k[x]$ where $Gal(f; k)$ acts transitively on f, but f is reducible.

Example: The answer requires a repeated root. The simplest example is x^2 over any field k. Certainly the only root is 0 so any group acts transitively on the roots – including our $Gal(x^2; k)$. Yet clearly x^2 is reducible. $\square$

41 Let K/k be a field extension. If $\alpha_1, \ldots, \alpha_n \in K$ are algebraically independent over k, and $\alpha \in k(\alpha_1, \ldots, \alpha_n) - k$, then α is transcendental over k.

Proof: Let $\alpha = \frac{p(\alpha_1,\ldots,\alpha_n)}{q(\alpha_1,\ldots,\alpha_n)}$ where $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$. Suppose α is algebraic over k; say it is a root of a polynomial $f(x) \in k[x]$. Then

Work of James, Dragos, and Dawn

$$f(\alpha) = a_0 + a_1 \frac{p(\alpha_1, \ldots, \alpha_n)}{q(\alpha_1, \ldots, \alpha_n)} + \cdots + a_m \frac{p(\alpha_1, \ldots, \alpha_n)^m}{q(\alpha_1, \ldots, \alpha_n)^m}.$$

So we clear the denominators and take

$$g(x) = q(\alpha_1, \ldots, \alpha_n) f(x).$$

However we may now take $g(x)$ to be a polynomial in $k(\alpha)[x_1, \ldots, x_n]$ in a natural way as:

$$g(\alpha)(x_1, \ldots, x_n) = q(x_1, \ldots, x_n) f(\alpha)(x_1, \ldots, x_n).$$

Notice then that $g(\alpha)(\alpha_1, \ldots, \alpha_n) = 0$. This means $\alpha_1, \ldots, \alpha_n$ is algebraically dependent over $k(\alpha)$. This implies $TrDeg(k(\alpha_1, \ldots, \alpha_n)/k(\alpha)) < n$.

Now by the Tower Law,

$$\begin{aligned} n &= TrDeg(k(\alpha_1, \ldots, \alpha_n) : k) = TrDeg(k(\alpha_1, \ldots, \alpha_n) : k(\alpha)) TrDeg(k(\alpha) : k) \\ &= TrDeg(k(\alpha_1, \ldots, \alpha_n)/k(\alpha)). \end{aligned}$$

However, we now have a contradiction as the transcendence degree cannot be both n and less than n. So α must be transcendental over k. $\square$

42 Let k be a field and x a transcendental element over k. Describe $Gal(k(x)/k)$.

There is a no resolution on a fully determined description of this extension's Galois group. Certain conditions on the fields, such as order, may exclude maps that here seem reasonable.

Example: We know any two transcendental extensions are isomorphic fields. Therefore given any two such elements α, β we can construct an automorphism sending α to β. $\square$

44 Let G be a finite group of automorphism of a field K with fixed field $k = K^G$. Show K/k is Galois and $Gal(K/k) = G$.

Proof: By Thm-2.7.3 we now $[K : k] = |G|$ so the extension is finite; furthermore, if $Gal(K/k) = G$ then by Thm-2.7.18 it follows K/k is normal and separable, and thus Galois. All we must show now is that $Gal(K/k) = G$.

Certainly $G \leq Gal(K/k)$, so we must now show these are all the elements. It follows $|G|[G^* : k] = |Gal(K/k)$ but notice that $G^* = k$ so $|G| = |Gal(K/k)$ and since all is finite the pigeon-hole-principle applies to say $G = Gal(K/k)$. $\square$

45 Show if K/k is a splitting field extension for $f \in k[x]$, then $[K : k] \leq (deg\ f)!$.

Proof: We know from exercise 19 that $[K : k] | (deg\ f)!$ so it is immediate. $\square$

46 If k is a field, $f \in k[x]$, and K/k is a splitting field then $[K : k] = (deg\ f)!$ implies f is separable and irreducible.

Thanks to Mike for the separability.

Proof: Suppose f has a repeated root α. Then there exists a $g(x) = k(\alpha)[x]$ and $f(x) = (x - \alpha)^2 g(x)$ – note we are guaranteed at least a factor of 2. Now it follows that $deg\ irr(\alpha; k) \leq deg\ f$ and $deg\ g = deg\ f - 2$. Thus using the result from exercise 45 it is now clear that

$$[K : k] = [K : k(\alpha)][k(\alpha) : k] \leq (deg\ f - 2)!(deg\ f) \neq (deg\ f)!$$

Whence f is must be separable to avoid contradictions.

We have $n = deg\ f$ roots so as the Galois group is characterized completely by its permutation on the roots it is clear $Gal(K/k)$ is embedded in S_n. As we know K/k is a separable normal extension it follows $n! = [K/k] = |Gal(K/k)|$ and so $Gal(K/k) = S_n$ by the pigeon-hole principle. This means the group is free to permute roots in any combination. However the group is also required to permute roots only within the irreducible factors. Thus the entire polynomial must be irreducible. $\square$

47 Compute $Gal(\mathbb{R}/\mathbb{Q})$.

Thanks to Hungerford and Dragos

Example: Take any automorphism $f : \mathbb{R} \to \mathbb{R}$. Such a map must be order preserving as: take $x \in \mathbb{Q}$, $x \geq 0$ then

$$f(x) = f(\sqrt{x}^2) = (f(\sqrt{x})^2 > 0.$$

Therefore as the positive set is preserved, order is preserved. Now take any $r \in \mathbb{R}$. For all $n \in \mathbb{N}$ it follows there exists a rational q such that $q < r < q+1/n$. Hence $f(q) = q < f(r) < f(q + 1/n) = q + 1/n$. As $n \to \infty$ we force $f(r) = r$. $\square$

48 Compute $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q})$.

Example: Because 2, 3, and 5 are prime we conclude x^2-2, x^2-3 and x^2-5 are all irreducible over $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{2},\sqrt{3})$ respectively; monic; and as they have degree 2 must be the corresponding polynomials $irr(\sqrt{2};\mathbb{Q})$, $irr(\sqrt{3};\mathbb{Q}(\sqrt{2}))$ and $irr(\sqrt{5};\mathbb{Q}(\sqrt{2},\sqrt{3}))$. As such each extension is of degree 2, and so the entire extension is of degree 8. In fact we now say $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ is the splitting field of $f(x)=(x^2-2)(x^2-3)(x^2-5)$. $f(x)$ is clearly separable, so the extension is Galois and hence $|Gal(f;\mathbb{Q})|=8$. Finally, the irreducible factors are all of degree 2 so each automorphism is an involution. Therefore it is the group $C_2\times C_2\times C_2$.

$\square$

49 Let K/k be a Galois extension, and L, M be intermediate fields. Denote by LM the minimal subfield of K containing L and M.

(i) Prove that $(L\cap M)^*=\langle L^*, M^*\rangle$.

(ii) Prove that $(LM)^*=L^*\cap M^*$.

(iii) Prove that $Gal(LM/L)\cong Gal(L/(L\cap M))$.

Proof: From the definition of a group join, we know

$$L^*\vee M^*=\bigcap_{L^*,M^*\leq H} H.$$

So if we apply our dual $*$ we get:

$$(L^*\vee M^*)^*=\bigcup_{L,M\geq H^*} H^*.$$

However we know $H^*\leq L\cap M$ whenever $H^*\leq L$ and M, as $L\cap M$ is the largest subfield contained in both L and M, and indeed $(L\cap M)^*$ is such an H, so $L\cap M=\bigcup_{L,M\geq H^*}H^*$, so in fact

$$(L^*\vee M^*)=((L^*\vee M^*)^*)^*=(L\cap M)^*.$$

Now consider $(LM)^*$. Given any $\sigma\in LM^*$ we know then σ fixes L and M so therefore $\sigma\in L^*\cap M^*$. Moreover this tells us

$$(LM)^*\leq L^*\cap M^*\leq L^*, M^*.$$

Applying the Galois correspondence we notice:

$$L, M\leq (L^*\cap M^*)^*\leq LM.$$

As $(L^*\cap M^*)^*$ is a field containing both L and M, and now visibly contained in the least such field, it must be precisely the field LM. Therefore $(LM)^*=(L^*\cap M^*)$.

Finally, let M/k be a normal extension. As such, M^* is normal in $G=Gal(K/k)$. Certainly then

$$L^*/(LM)^*=L^*/(L^*\cap M^*)\cong L^*M^*/M^*=(L\cap M)^*/M^*$$

by the second isomorphism theorem for groups. But notice $L^*/(L^*\cap M^*)=Gal(LM/L)$ and $L^*M^*/M^*=Gal(M/L\cap M)$; thus, $Gal(LM/L)\cong Gal(M/L\cap M)$. $\square$

Example: When L/k is not normal, it is possible that $Gal(LM/L)$ not be isomorphic to $Gal(L/L\cap M)$. For instance, take $p(x)$ to be a polynomial over $\mathbb{Q}$ whose Galois group in splitting field K is isomorphic to A_4. There must correspond subfield L and M which correspond to the subgroups $L^*=A_3$ and $M^*=\langle(12)(34)\rangle$ respectively. Thus $(LM)^*=L^*\cap M^*=\mathbf{1}$ and $(L\cap M)^*=L^*\vee M^*=A_4$. Notice then that

$$[LM:L]=[L*:(LM)^*]=3, \qquad [L:L\cap M]=[(L\cap M)^*:L^*]=4.$$

Since $|Gal(LM/L)|=[LM:L]$ and $|Gal(L/L\cap M)|=[L:L\cap M]$ it follows these groups cannot be isomorphic as they do not even have the same order. $\square$

50 Let k be a subfield of $\mathbb{R}$ and $f\in k[x]$ an irreducible cubic with discriminant D. Then

(i) $D>0$ if and only if f has three real roots;

(ii) $D<0$ if and only if f has precisely one real root.

Proof: We take a result from analysis that states every cubic equation over $\mathbb{R}$ has one real root. Therefore f has either three roots in $\mathbb{R}$ or only one, as complex roots must come in conjugate pairs. When $D=0$ it follows we have a repeated root. This would imply the f is inseparable polynomial over a characteristic 0 field, an impossibility. Therefore it suffices to show $D>0$ if and only if f has only real roots and the second result will follow by the contrapositive in both directions, together with $D\neq 0$ and the existence of only one or three real roots.

Let $a_1\in\mathbb{R}$ be the one real root, and a_2+ib_2 and a_2-ib_2 be the two conjugate roots in $\mathbb{C}$ (possibly they are in $\mathbb{R}$ as well).

$$\begin{aligned} D &= (a_1-(a_2+ib_2))^2(a_1-(a_2-ib_2))^2((a_2+ib_2)-(a_2-ib_2))^2 \\ &= (((a_1-a_2)-ib_2))((a_1-a_2)+ib_2))(2ib_2))^2 \\ &= ((a_1-a_2)^2+b_2^2)^2(2ib_2)^2 \end{aligned}$$

Now we see the discriminant is positive if and only if $b_2=0$ which occurs if and only if all roots are real. $\square$

51 Let $char\ k\neq 2$ and $f\in k[x]$ a cubic whose discriminant has a square root in k, then f is either irreducible or splits in k.

Proof: If f has no multiple roots then by virtue of having a square root of the discriminant in k, and $char\ k\neq 2$, we know $Gal(f;k)\leq A_3$. Thus, the Galois group is trivial implying f splits in k, or it is A_3 implying there are no roots of f in k (refer to Exercise-13, we have a transitive action on the roots of a polynomial with no multiple roots so it is irreducible.)

Now for the cases when f has multiple roots. If $f(x)=(x-\alpha)^3$, then certainly it splits in k if and only if $\alpha\in k$, so when $\alpha\notin k$ it is irreducible. Suppose $f(x)=(x-\alpha)^2(x-\beta)$ in some splitting field. If $\alpha\in k$ then it follows $\beta\in k$ as the only extension of a monomial is trivial. Now suppose $\alpha\notin k$. If β is also not in k then by the definition f is irreducible over k. Suppose instead $\beta\in k$. Then $(x-\alpha)^2$ is irreducible over k. If k has characteristic 0, then there are no inseparable polynomials so $\alpha\in k$ causing a contradiction. In the final case, k has characteristic greater than 2 by assumption. Since the characteristic is greater than the degree of the polynomial, the polynomial cannot be inseparable as the derivative test will not be 0. Therefore $(x-\alpha)^2$ should be separable which it visibly is not. Thus this case cannot exist for any k with characteristic not equal to 2. □

52 Let f be an irreducible separable quartic over a field k and α be a root of f. There is no field properly between k and $k(\alpha)$ if and only if the Galois group of f is A_4 or S_4.

Proof: Let K be splitting field for f over k. As such the extension is Galois. Therefore the intermediate fields correspond precisely to intermediate subgroups. Since f is irreducible it follows $[k(\alpha):k]=4$. Also the automorphisms need to act transitively on the 4 roots so it is in fact the case that the Galois group is V, C_4, D_8, A_4 or S_4.

The first three are 2-groups. However we know from the first Sylow theorem that every 2-subgroup lies inside a 4-subgroup of any 8-group. Thus none of these groups of a subgroup of index 4 with no intermediate group. Therefore the corresponding field extension with these Galois groups will have no such case where $[k(\alpha):k]=4$ and there are no intermediate fields.

This leaves S_4 and A_4. All we need to do is confirm they have subgroups of index 4 with no intermediate subgroups. This follows empirically by noticing S_3 in S_4 and A_3 in A_4. If S_3 is contained in an intermediate subgroup, this subgroup must have order 12. However there is only one order 12 subgroup of S_4 which is A_4. Moreover, S_3 is not in A_4 as A_4 does not contain any subgroup of order 6. This last statement in fact also explains why there are no intermediate subgroups between A_3 and A_4. Therefore both S_4 and A_4 are candidates for such a situation. □

53 Every element of a finite field can be expressed as a sum of two squares.

Proof:

□

54 Determine the Galois group of x^3+11 over $\mathbb{Q}$, determine all subfields of its splitting field, and decide which are normal over $\mathbb{Q}$. Describe the subfields by their generators.

Proof: The polynomial splits as

$$(x-\sqrt[3]{11})(x^2-\sqrt[3]{11}x+\sqrt[3]{11^2}).$$

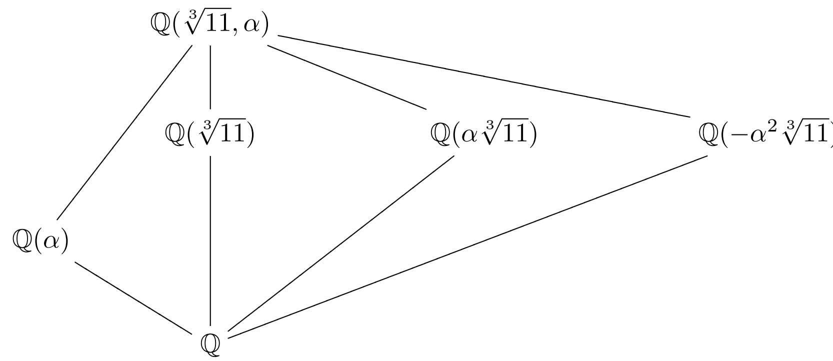
Therefore letting $\alpha=\frac{1}{2}-i\frac{\sqrt{3}}{2}$ we have α and $-\alpha^2$ as roots of x^2-x+1. So we have a splitting extension of $\mathbb{Q}(\sqrt[3]{11},\alpha)/\mathbb{Q}$. The degree is equal to

$$[\mathbb{Q}(\sqrt[3]{11},\alpha):\mathbb{Q}(\sqrt[3]{11})][\mathbb{Q}(\sqrt[3]{11}):\mathbb{Q}]=2\cdot 3=6$$

as x^3+11 is irreducible over $\mathbb{Q}$ and the roots of x^2-x+1 are complex so it is irreducible over $\mathbb{Q}(\sqrt[3]{11})$.

Since x^3+11 is irreducible, its Galois group is a transitive group on all irreducible components – here there is only one (there can only ever be one with any irreducible degree 3 polynomial: you cannot split only three elements into non-trivial imprimitivity blocks.) The only group of order 6 that acts transitively on 3 elements is S_3 so the Galois group is S_3.

The intermediate fields are exhibited as



Certainly every subfield is normal in $\mathbb{Q}(\sqrt[3]{11}, \alpha)$ as it is a splitting field – moreover it corresponds to the trivial group which is normal in all subgroups. Finally we should expect to observe the $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal. This is true in two ways: first it is the splitting field for $x^2 - x + 1$, and second it is of degree 2. We also observe the remaining intermediate fields are not normal as in each case, the polynomial $x^3 + 11$ does not split in them even though each contains a root of $x^3 + 11$.

To be certain of our construction we must verify the automorphism exist that correspond to this field extension. Define $\sigma(\sqrt[3]{11}) = -\alpha^2\sqrt[3]{11}$ and leaving α invariant. By the fact that both are roots of the same monic minimal degree irreducible polynomial, we know there exists a field monomorphism σ and as it lies inside a normal extension we may extend this to $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[3]{11}, \alpha)$. Notice then

$$\sigma(\alpha\sqrt[3]{11}) = \sigma(\alpha) - \alpha^2\sqrt[3]{11} = -\alpha^3\sqrt[3]{11} = \sqrt[3]{11},$$

$$\sigma(\alpha^2\sqrt[3]{11}) = -\alpha^4\sqrt[3]{11} = \alpha\sqrt[3]{11},$$

so that in fact $\sigma = (\sqrt[3]{11}, -\alpha^2\sqrt[3]{11}, \alpha\sqrt[3]{11})$. Therefore σ has order 3 – it is A_3 – and it fixes $\mathbb{Q}(\alpha)$ as predicted.

In similar fashion, $\tau(\sqrt[3]{11}) = \sqrt[3]{11}$ and $\tau(\alpha) = -\alpha^2$ again produces a monomorphism of

$$\mathbb{Q}(\alpha, \sqrt[3]{11})/\mathbb{Q}(\sqrt[3]{11}) \to \mathbb{Q}(-\alpha^2, \sqrt[3]{11})$$

by the fact that α and $-\alpha^2$ share the same monic minimal degree irreducible polynomial. Clearly this is an automorphism of $\mathbb{Q}(\alpha, \sqrt[3]{11})$. Furthermore, $\tau = (\alpha\sqrt[3]{11}, -\alpha^2\sqrt[3]{11})$ so τ has order 2, and fixes $\mathbb{Q}(\sqrt[3]{11})$ so the correspondence is verified. $\square$

56 Find all subfields of the splitting field for $x^3 - 7$ over $\mathbb{Q}$. Determine its Galois group, and which subfields are normal.

Proof: The polynomial splits as

$$(x - \sqrt[3]{7})(x^2 + \sqrt[3]{7}x + \sqrt[3]{7^2}).$$

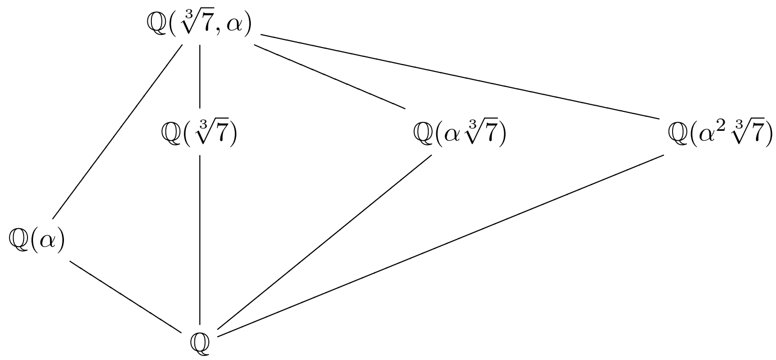
Therefore letting $\alpha = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ then α and α^2 are the roots of $x^2 - x + 1$; whence, we have a splitting extension of $\mathbb{Q}(\sqrt[3]{7}, \alpha)/\mathbb{Q}$. The degree is equal to

$$[\mathbb{Q}(\sqrt[3]{7}, \alpha) : \mathbb{Q}(\sqrt[3]{7})][\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 2 \cdot 3 = 6$$

as $x^3 + 7$ is irreducible over $\mathbb{Q}$ and the roots of $x^2 - x + 1$ are complex so it is irreducible over $\mathbb{Q}(\sqrt[3]{7})$.

Since x^3+7 is irreducible, its Galois group is a transitive group on 3 elements with order 6 – it is S_3.

The intermediate fields are exhibited as



Certainly every subfield is normal in $\mathbb{Q}(\sqrt[3]{7},\alpha)$ as it is a splitting field – moreover it corresponds to the trivial group which is normal in all subgroups. Finally we should expect to observe the $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal. This is true in two ways: first it is the splitting field for x^2+x+1, and second it is of degree 2. We also observe the remaining intermediate fields are not normal as in each case, the polynomial x^3+7 does not split in them even though each contains a root of x^3+7.

To be certain of our construction we must verify the automorphism exist that correspond to this field extension. Define $\sigma(\sqrt[3]{7})=\alpha\sqrt[3]{7}$ and leaving α invariant. By the fact that both are roots of the same monic minimal degree irreducible polynomial, we know there exists a field monomorphism σ and as it lies inside a normal extension we may extend this to $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[3]{7},\alpha)$. Notice then

$$\sigma(\alpha\sqrt[3]{7})=\sigma(\alpha)\alpha\sqrt[3]{7}=\alpha^2\sqrt[3]{7}$$

so that in fact $\sigma=(\sqrt[3]{7},\alpha\sqrt[3]{7},\alpha^2\sqrt[3]{7})$. Therefore σ has order 3 – it is A_3 – and it fixes $\mathbb{Q}(\alpha)$ as predicted.

In similar fashion, $\tau(\sqrt[3]{7})=\sqrt[3]{7}$ and $\tau(\alpha)=\alpha^2$ again produces a monomorphism of

$$\mathbb{Q}(\alpha,[3]7)/\mathbb{Q}(\sqrt[3]{7})\to\mathbb{Q}(\alpha^2,\sqrt[3]{7})$$

by the fact that α and α^2 share the same monic minimal degree irreducible polynomial. Clearly this is an automorphism of $\mathbb{Q}(\alpha,\sqrt[3]{7})$. Furthermore, $\tau=(\alpha\sqrt[3]{7},\alpha^2\sqrt[3]{7})$ so τ has order 2, and fixes $\mathbb{Q}(\sqrt[3]{7})$ so the correspondence is verified. $\square$

57 Let K be a splitting field for x^4+6x^2+5 over $\mathbb{Q}$. Find all subfields of K.

Proof: Notice

$$x^4+6x^2+5=(x^2+1)(x^2+5)=(x-i)(x+i)(x-i\sqrt{5})(x+i\sqrt{5}),$$

and, $irr(i;\mathbb{Q})=x^2+1$ and $irr(i\sqrt{5};\mathbb{Q})=x^2+5$. Thus we have know our splitting field to be $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}$. Moreover, its degree is 4 as $deg\ irr(\sqrt{5};\mathbb{Q})=2$ and as all the roots of x^2+1 are complex, it is irreducible over $\mathbb{Q}(\sqrt{5})$ we obtain the tower of extensions:

$$[\mathbb{Q}(i,\sqrt{5}):\mathbb{Q}]=[\mathbb{Q}(i,\sqrt{5}):\mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}):\mathbb{Q}]=4.$$

Since the irreducible factors each contain only two of the roots it follows the Galois group lies in S_4 but it not transitive on the four elements. There is only one such family of subgroups in S_4, the Klein-4-groups of the form:

$$K_4^1 = \{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}.$$

So this is our Galois group:

$$G = \{(i), (i\ \ -i), (i\sqrt{5}\ \ -i\sqrt{5}), (i\ \ -i)(i\sqrt{5}\ \ -i\sqrt{5})\}.$$

Note the automorphisms exist and are well-defined as they are clearly the extension of the $\mathbb{Q}$-monomorphisms $i \to -i$ etc. which have the same irreducible polynomial so they are justified.

Hence the subfields of K correspond to this lattice. Having the automorphisms in hand we can compute the subfields as

$$\begin{tikzcd}
 & \mathbb{Q}(i,\sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i) \arrow[dr, dash] & \mathbb{Q}(\sqrt{5}) \arrow[d, dash] & \mathbb{Q}(i\sqrt{5}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

In particular, $\mathbb{Q}(i)$ is the fix field of $\sigma(i) = i$ and $\sigma(\sqrt{5}) = -\sqrt{5}$, which is to say $\sigma = (i\sqrt{5}, -i\sqrt{5})$; $\mathbb{Q}(\sqrt{5})$ is fixed in $\tau = (i, -i)$; and finally $\mathbb{Q}(i\sqrt{5})$ is fixed by $(i\ \ -i)(i\sqrt{5}\ \ -i\sqrt{5})$, as $i\sqrt{5} \to -i\sqrt{5} \to i\sqrt{5}$. All are normal as $\mathbb{Q}(i)$ is the splitting field of x^2+1, $\mathbb{Q}(\sqrt{5})$ of x^2-5 and $\mathbb{Q}(i\sqrt{5})$ that of x^2+5. $\square$

58 Let K be a splitting field for $x^4 - 3$ over $\mathbb{Q}(i)$. Find the Galois group of K over $\mathbb{Q}(i)$.

Proof:

$$x^4 - 3 = (x^2 - \sqrt{3})(x^2 + \sqrt{3}) = (x - \sqrt[4]{3})(x + \sqrt[4]{3})(x - i\sqrt[4]{3})(x + i\sqrt[4]{3}).$$

Therefore $\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q}(i)$ is a splitting field. Moreover, as $\sqrt[4]{3} \notin \mathbb{Q}(i)$ it follows $x^4 - 3$ is irreducible over $\mathbb{Q}(i)$. Moreover, the irreducible factors are not over $\mathbb{Q}(i)$ so there is only one irreducible component and thus the Galois group acts transitively on all four roots.

The degree of the extension is 4 as the $irr(\sqrt[4]{3}; \mathbb{Q}(i)) = x^4 - 3$. Therefore the Galois group is V or C_4. There is however only one intermediate field: $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}(i)$. So it must be C_4. $\square$

59 Let $\varepsilon \in \mathbb{C}$ be a primitive 7th root of unity. Determine the minimal polynomial of ε, the structure of the Galois group, and the subfields.

Work with Dawn.

Proof: We know $\frac{x^p - 1}{x - 1}$ is irreducible over $\mathbb{Q}$ and certainly this is nothing more than Φ_7 so it has ε as a root. Now the Galois group of a Cyclotomic extension is cyclic (mostly by design) so it must be the cyclic group C_6. Therefore we expect to find two proper intermediate fields.

To formalize the Galois group we can take σ_k as a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ with $e^{2\pi i/7} \mapsto e^{2\pi ik/7}$ and $k \in \mathbb{Z}_7^{\times}$. The automorphism is σ_1 is unit and σ_3 is a generator. From here we identify the intermediate fields as $\langle\sigma_2\rangle^*$ and $\langle\sigma_6\rangle^*$. $\square$

60 Let $K = \mathbb{Q}(i, e^{2\pi i/3})$, where $i = \sqrt{-1}$ in $\mathbb{C}$. Find $[K : \mathbb{Q}]$ and determine $Gal(K/\mathbb{Q})$.

Example: The polynomial $\frac{x^3-1}{x-1}$ has roots $-\frac{1}{2} \pm i\sqrt{3}2$. Certainly $\sqrt{3} \notin \mathbb{Q}(i)$ so $\Phi_3(x) = \frac{x^3-1}{x-1}$ is irreducible over $\mathbb{Q}(i)$. Hence $[K : \mathbb{Q}] = [K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot 2 = 4$. Moreover, the extension is no visibly a splitting field of $(x^2+1)\Phi_3(x)$ so it is normal, and as $\mathbb{Q}$ has characteristic 0 also separable; therefore, the extension is Galois. Moreover, the Galois group must act transitively on the irreducible factors, which are $x^2 + 1$ and $\Phi_3(x)$ respectively. As both of these have only two roots we see that no automorphism in $Gal(K/\mathbb{Q})$ can have order greater than 2 (they are all transpositions when restricted to the roots of the irreducible factors). As there are only two groups of order 4, we must conclude the Galois group of the extension is $C_2 \times C_2$ as C_4 has elements of order 4. In particular

$$Gal(K/\mathbb{Q}) = \langle (i, -i), (e^{2\pi i/3}, e^{4\pi i/3}) \rangle.$$

□

68 In a field of characteristic p, there is one p^m-th root of unity.

Proof: By the Freshman's dream we know

$$x^{p^m} - 1 = (x-1)^{p^m}.$$

Hence this polynomial has only one root, so there is at most one p^m-th root of unity. Each certainly has at least one root of unity – simply 1. Thus there is precisely one p^m-th root of unity. □

72 If F is a finite field and $f \in F[x]$ is irreducible then $f'(x) \neq 0$.

Proof: Let F have characteristic $p > 0$, which it must have as it is a finite field.

Suppose $f'(x) = 0$. Then there exists some $g(x) \in F[x]$ such that $f(x) = g(x^p)$ (this way the non-zero coefficients are annihilated.) Now F is a finite field so the Frobenius map $a \mapsto a^p$ is an automorphism of F. Therefore every element has a p-th root in F – we will denote such a root as $\sqrt[p]{a}$. In this way we see:

$$\begin{aligned} g(x^p) &= a_0 + a_1 x^p + \cdots + a_n x^{pn} \\ &= (\sqrt[p]{a_0})^p + (\sqrt[p]{a_1})^p x^p + \cdots + (\sqrt[p]{a_n})^p x^{pn} \\ &= (\sqrt[p]{a_0} + \sqrt[p]{a_1} x + \cdots + \sqrt[p]{a_n} x^n)^p \\ &= (f_2(x))^p. \end{aligned}$$

Visibly $f(x)$ is reducible as $p > 1$. As all other polynomials have non-zero derivatives it follows any irreducible polynomial over F has non-zero derivative.
□

77 Show there is a Galois extension of $\mathbb{F}_{125}$ with Galois group C_6.

Example: Notice $125 = 5^3$ so we begin by acknowledging $\mathbb{F}_{5^{18}}$ exists as it is the splitting field of $x^{5^{18}} - x$ over $\mathbb{F}_5$. Now as $3|18$ we have $\mathbb{F}_{125} \leq \mathbb{F}_{3,814,697,265,625}$. Moreover, the degree of $[\mathbb{F}_{125} : \mathbb{F}_5] = 3$ so $[\mathbb{F}_{3,814,697,265,625} : \mathbb{F}_{125}] = 6$. As the Galois group of $\mathbb{F}_{3,814,697,265,625}/\mathbb{F}_5$ is C_{18}, the subgroups are all cyclic, so the Galois group of $\mathbb{F}_{3,814,697,265,625}/\mathbb{F}_{125}$ is C_6. □

78 Every Galois extension of $\mathbb{C}$ is Galois over $\mathbb{R}$.

Proof: Every Galois extension is finite, so it is algebraic. However $\mathbb{C}$ is algebraically closed so there are only trivial Galois extensions. Therefore the question is equivalent to asking if $\mathbb{C}$ is a Galois extension of $\mathbb{R}$. Certainly so as it has degree 2 which is both finite and also indicates normal, and it is over a field of characteristic 0 so it is separable. $\square$

80 Let k be a subfield of an algebraically closed field K such that the transcendence degree is finite. Prove that if $\varphi : K \to K$ is a k-monomorphism, then φ is an automorphism of K.

Proof: Let $T = \{a_1, \dots, a_n\}$ be a transcendence basis of K. Since φ is a monomorphism it follows $\varphi(T)$ is a set with cardinality n. Moreover, if $\varphi(T)$ is algebraically dependent, then there exists some $p(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$ such that $p(\varphi(a_1), \dots, \varphi(a_n)) = 0$. Since $\varphi|_{k(T)}$ is bijective, fixing k, we see that

$$0 = \varphi^{-1}(0) = \varphi^{-1}(p(\varphi(a_1, \dots, \varphi(a_n)) = p(a_1, \dots, a_n).$$

This contradicts the assumption that T is algebraically independent. Whence we now see $\varphi(T)$ is as well. Since it has the same size as the transcendence degree it follows $\varphi(T)$ is a transcendence basis for K. Therefore indeed we now see that φ is an automorphism of $k(T)$ – the purely transcendental extension of k in K. Now we look to the algebraic material.

We know that any $k(T)$-monomorphism of $k(T)(\alpha)$ lies in $k(T)(\beta)$ where α and β are roots of the same irreducible. Therefore $\varphi|_{k(T)(A)}$ is an automorphism of $k(T)(A)$ for any set A of all roots of any given irreducible. Since K is algebraically closed, we know $K/k(T)$ is precisely the extension of adjoining all roots, so in fact φ is an automorphism of all of K. $\square$

83 Let $f \in \mathbb{F}_p[x]$ such that $f' = 0$, then any splitting field for f is separable.

Proof: Let α be any element in the splitting field and take $g(x)$ to be $irr(\alpha; k)$. If the extension is to be inseparable then we may suppose that $g(x)$ is an example of an inseparable polynomial that makes it so. However, for $g(x)$ to be inseparable it must have a 0 derivative. Whence $g(x)$ is irreducible if and only at least one coefficient has no p-th root in k. However k is a finite field of characteristic p. Therefore the Frobenius map is an automorphism, so every element has a p-th root in k. This leads to a contradiction: either $g(x)$ is reducible – impossible by the choice of $g(x)$, or it is separable. So it must be separable, and now as every minimal polynomial is separable, the extension is separable. $\square$

84 A field of order 243 contains exactly one proper subfield.

Proof: First factor 243 into 3^5. Since the existence of intermediate fields is purely a number theory game we quickly notice since 5 is prime, the only divisors are 1 and 5, so the only subfield is $\mathbb{F}_3$ and in fact $\mathbb{F}_{243}$ has only one proper subfield. $\square$

85 Give an example of a finite extension $K/\mathbb{F}_q$ in which two intermediate fields L and M are incomparable.

Example: The smallest such example comes from extending $\mathbb{F}_q$ to $\mathbb{F}_{q^6}$. Because of the extension has Galois group C_6 (simply because the degree of the extension is 6, and the Galois group of a finite field extension of a finite field must be cyclic.) The group C_6 has two incomparable subgroups – one of order 2, another of order 3 – so there is precisely the same correspondence in the subfields. $\square$

86 Prove in a finite extension of a finite field every intermediate field is stable (every automorphism of the intermediate field maps back into the subfield.)

Proof: The Galois group of any such extension must be cyclic. As such every subgroup is normal. Normal subgroups imply normal intermediate fields. If an intermediate field extension is normal then it stable. $\square$

88 Show the field extension $\mathbb{Q}(x)/\mathbb{Q}(x^6)$ is not a Galois extension.

Example: Consider the polynomial $y^6 - x^6 \in \mathbb{Q}(x^6)[y]$. Certainly x is a root, and furthermore we can factor $y^6 - x^6$ as

$$(y-x)(y+x)(y^2-yx+x^2)(y^2+yx+x^2).$$

Since we are over $\mathbb{Q}$ we can apply the quadratic formula to solve for the remaining factors:

$$y = \frac{\pm x \pm \sqrt{-3x^2}}{2}.$$

Now we notice that the remaining roots are complex so their monomials are not over $\mathbb{Q}(x^6)$. Now by inspection:

$$\begin{array}{rcl}
(y-x)(y+x) & = & y^2 - x^2 \notin \mathbb{Q}(x^6) \\
(y-x)(y^2+yx+x^2) & = & y^3 - x^3 \notin \mathbb{Q}(x^6) \\
(y-x)(y^2-yx+x^2) & = & y^3 - 2y^2x + 2yx^2 - x^3 \notin \mathbb{Q}(x^6) \\
(y+x)(y^2+yx+x^2) & = & y^3 + 2y^2x + 2yx^2 + x^3 \notin \mathbb{Q}(x^6) \\
(y+x)(y^2-yx+x^2) & = & y^3 + x^3 \notin \mathbb{Q}(x^6) \\
(y^2+yx+x^2)(y^2-yx+x^2) & = & y^4 + y^2x^2 + x^4 \notin \mathbb{Q}(x^6).
\end{array}$$

Therefore $y^6 - x^6$ is irreducible as none of its proper factors is over $\mathbb{Q}(x^6)$ and none of the roots are in $\mathbb{Q}(x^6)$. However this illustrates that the extension is not Galois as it does not contain any of the complex roots but it does contain some roots, so the extension is not normal, hence, not Galois. $\square$

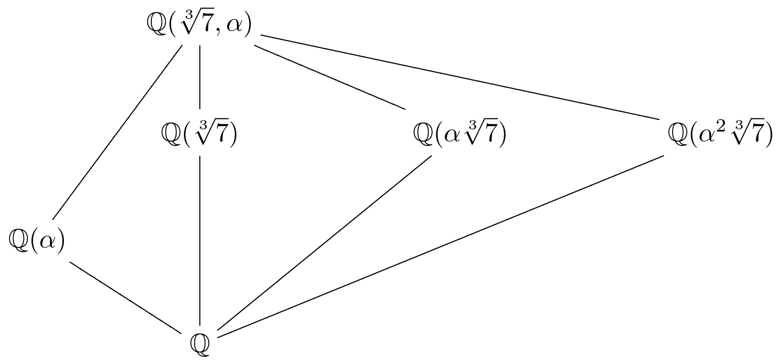
89 Let K/k be a finite field extension and L, M be intermediate fields such that $L \cap M = k$. Prove $[LM : k] \leq [L : k][M : k]$ and show by example that a strict inequality is possible.

Proof: Notice $LM = L(M)$; whence, $[LM : k] = [LM : L][L : k]$. Now extend a basis from the linearly independent set $\{1\}$ for the vector space LM over L. This basis $A = \{1 = a_1, a_2, \dots, a_m\}$ if finite since we lie in a finite field extension. Moreover, if any two basis vectors lie in L then they are linearly dependent so in fact all $A \subset M - L \cup \{1\}$ since the only element from L is the vector 1. Therefore $[LM : L] \leq [M : L \cap M]$ Now recall $L \cap M = k$, so $[LM : L] \leq [M : L \cap M] = [M : k]$. Therefore we now observe that:

$$[LM : k] \leq [M : k][L : k].$$

$\square$

Example: Consider the splitting field in $\mathbb{C}$ of $x^3 - 7$ over $\mathbb{Q}$. We have already established that this possess the intermediate fields:



Notice then the intermediate fields $L=\mathbb{Q}(\sqrt[3]{7})$ and $M=\mathbb{Q}(\alpha\sqrt[3]{7})$ intersect at $\mathbb{Q}$ and join at $\mathbb{Q}(\sqrt[3]{7},\alpha)$. Therefore

$$6=[LM:\mathbb{Q}]\leq 9=[L:\mathbb{Q}][M:\mathbb{Q}].$$

□

91 Let k be a field, $p(x)$ an irreducible polynomial in $k[x]$ of degree n, and let K be a Galois extension of k containing a root α of $p(x)$. Let $G=Gal(K/k)$, and G_α be the set of all $\sigma\in G$ with $\sigma(\alpha)=\alpha$.

(a) Show that G_α has index n in G.

(b) Show that if G_α is normal in G, then $p(x)$ splits in the fixed field of G_α.

Proof: To begin with, given any two $\sigma,\tau\in G_\alpha$ it follows $\sigma(\alpha)=\alpha$ and $\tau(\alpha)=\alpha$ so $\sigma\tau(\alpha)=\sigma(\alpha)=\alpha$ so $\sigma\tau\in G_\alpha$. Naturally $1(\alpha)=\alpha$ so $1\in G_\alpha$. Finally $\alpha=\sigma^{-1}(\sigma(\alpha))=\sigma^{-1}(\alpha)$ by the definition of functional inverses, so $\sigma^{-1}\in G_\alpha$ and so Γ_α is a subgroup of G.

Of importance is the fact the K is a Galois extension over k. Thus it is normal and finite, so G is finite and $p(x)$ splits in K as it contains one root in K. Therefore G contains the Galois group of $p(x)$.

Notice $p(x)$ has degree n and is irreducible so $[k(\alpha):k]=n$. As G_α fixes α and all of k it is certainly contained in $k(\alpha)^*$. Now we must show this is sufficient. Given any σ which fixed $k(\alpha)$ it follows $\sigma(\alpha)=\alpha$ so indeed $\sigma\in G_\alpha$. Therefore $G_\alpha=k(\alpha)^*$. As such the by the Galois correspondence we know $[G:G_\alpha]=[k(\alpha):k]=n$.

Now suppose G_α is normal in G. Then as $G_\alpha=k(\alpha)^*$ and the extension is Galois it follows * is invertible so $G_\alpha^*=k(\alpha)$, so $k(\alpha)$ is normal over k. As it contains one root of $p(x)$ it must contain all roots, so $p(x)$ splits in $k(\alpha)$. □

92 Let $k(\alpha)/k$ be a field extension obtained by adjoining a root α of an irreducible separable polynomial $f\in k[x]$. Then there exists an intermediate field $k<F<k(\alpha)$ if and only if the Galois group $Gal(f;k)$ is imprimitive. If the group is imprimitive then the subfield F can be chosen so that $[F:k]$ is equal to the number of imprimitivity blocks.

Proof: If the Galois group is primitive then it has maximal stabilizer of α. However G_α determines the field $k(\alpha)$ (see 91) that is now minimal over k, so there is no intermediate field. Whence in the contrapositive if an intermediate field exists then G is imprimitive.

Now suppose G acts imprimitively on the roots of f. Then there is a non-trivial block decomposition of the roots, one of which contains α, call this block B. Every element that stabilizes α must also act inside the block of B. Furthermore, G acts transitively inside B so there exists and element $g \in G$ such that $g\alpha = \beta$ for some distinct $\beta \in B$. Therefore G_B – the elements that act inside of B (perhaps stabilize B is the proper term, only they are not actually fixing elements of B) – is a proper parent group of G_α. As such it corresponds to and intermediate field $k < G_B^* < G_\alpha^*$. Moreover we now see that the index $[G : G_B]$ is the number of imprimitivity blocks so we have the required field whose extension degree is the number of imprimitivity blocks. $\square$

Chapter 3

Modules

---

1 Noetherian/Artinian Rings. Let K be an infinite field extension of k. Let R be the ring of all 2×2 upper triangular matrices:

$$\begin{pmatrix} \alpha & \beta \\ 0 & c \end{pmatrix}$$

with $\alpha, \beta \in K$ and $c \in k$. Show that R is left artinian and left noetherian but is neither right artinian nor right noetherian.

Example: The submodules of ${}_R R$ are nothing more than the left ideals of R as left translation must be closed in each submodule. Given any ideal S of R, we take $A \in S$ and $B \in R$ and observe:

$$BA = \begin{pmatrix} \alpha & \beta \\ 0 & c \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' & \alpha\beta' + \beta c' \\ 0 & cc' \end{pmatrix}.$$

As A comes from an ideal S, then BA is in S. The multiplication above demonstrates that the projection maps $\pi_{1,1} : R \to K$ and $\pi_{2,2} : R \to k$ are ring homomorphisms (the addition is clearly preserved) and so they tell us that

$$\pi_{1,1}(BA) \in \pi_{1,1}(S); \qquad \pi_{2,2}(BA) \in \pi_{2,2}(S).$$

Indeed, $\pi_{1,1}(S)$ is an ideal of K and $\pi_{2,2}(S)$ is an ideal of k. As both K and k are fields we have only the trivial choices of ideals. Therefore the components $A_{1,1}$ and $A_{2,2}$ correspond to the two ideals of their respective fields which gives us an up bound of four choices for the ideals in these components.

However, the component $(BA)_{1,2}$ illustrates the fact that the projection map $\pi_{1,2} : R \to K$ is not a ring homomorphism as multiplication is not preserved.

So now we know we may take

$$S = \begin{bmatrix} I & T \\ 0 & J \end{bmatrix}$$

where $I \trianglelefteq K$ and $J \trianglelefteq k$, and T a subset of K closed under addition and with the property that $KT + KJ \subseteq T \subseteq K$. If $J = k$ then

$$KJ = Kk = K \leq T \subseteq K; \qquad T = K.$$

So assume we have $J = 0$. Then we simply have the requirement that $KT \subseteq T \subseteq K$, and I does not factor into the problem at all. Clearly then $0 \in T$ if T is non-empty – which it must be as otherwise matrices in S would not have an upper right corner. Moreover, if there is a non-zero element $a \in T$, then $a^{-1} \in K$ so $1 \in T$ and then from here clearly $K \subseteq T \subseteq K$ forcing once again $T = K$. Thus we have the following list of left ideals:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} K & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & K \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} K & K \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & K \\ 0 & k \end{bmatrix}, \quad \begin{bmatrix} K & K \\ 0 & k \end{bmatrix}.$$

As there are only finitely many left ideals, the ring is trivially left artinian and left noetherian.

Now consider the right ideals. Given K/k is infinite, it follows there is a basis $B = \{b_i : i \in I\}$ for K/k as a vector space which is infinite. Certainly $k_n = Span_k\{b_0, \ldots, b_n\}$ is an infinite ascending chain of distinct k-vector spaces in K. Moreover, this induces the same in the R_R:

$$S_n = \begin{pmatrix} 0 & k_n \\ 0 & 0 \end{pmatrix}.$$

Therefore R_R is not right noetherian. With the similar construction: $k'_n = Span_k\{B_i\ : i \in I\backslash\{0,\dots,n\}\}$ we see R_R is neither right artinian as this is an infinite descending chain.[1] $\square$

2 D.C.C. submodules and quotients. Let V be a left R-module and $W \leq V$ be a submodule. Then V satisfies the D.C.C. if and only if W and V/W do.

Hint: Use the correspondence theorem and the second isomorphism theorem.

Proof: Suppose V satisfies the D.C.C. Given any chain of submodules in W, certainly these are submodules of V so they stabilize in finitely many steps in V, and so too in W. Likewise, given any chain of submodules in V/W, by the correspondence theorem we have a chain of submodules in V whose factors are the original chain in V/W. Thus in V they stabilize so in V/W they stabilize.

Now suppose V/W and W satisfy the D.C.C. Take a chain

$$V_0 \geq V_1 \geq \cdots$$

in V. This induces the chains:

$$V_0 + W/W \geq V_1 + W/W \geq \cdots ; \qquad V_0 \cap W \geq V_1 \cap W \geq \cdots .$$

As both V/W and W satisfy the D.C.C. it follows both these chains stabilize. Now we use the 2nd isomorphism theorem to replace our chain in V/W with:

$$V_0/V_0 \cap W \geq V_1/V_1 \cap W \geq \cdots ,$$

which must also stabilize in finitely many steps as it is isomorphic to the chain in V/W. Since the quotients and the intersections stabilize, and we have an abelian group, the original chain stabilizes. $\square$

3 Modules over artinian Rings. If R is left artinian and V is a finitely generated left R-module then V satisfies D.C.C.

Hint: Resolve the module with a finitely generated free R-module, then use Exercise-3.2.

Proof: Given V is finitely generated, it follows it has a generating set $\{a_1, \dots, a_n\}$, and so the free module R^n maps canonically onto V. Therefore V is a quotient module of R^n. However, from Exercise-3.2 we know if R^n satisfies D.C.C., then so must the quotient V. Therefore we need only prove R^n satisfies D.C.C.

Given R is left artinian we know every chain of left ideals in R has finite length. In $R \oplus R$ we have the canonical embedding $R \oplus \mathbf{0}$ of R, and we notice that by projecting we obtain $R \oplus R/R \oplus \mathbf{0} \cong R$. Hence, using Exercise-3.2 in reverse we see that R^2 satisfies the D.C.C. as a left R-module. Now we induct. Let R^k satisfy the descending chain condition. As such, $R^{k+1}/R^k \oplus \mathbf{0} \cong R$ so once again by Exercise-3.2 we know R^{k+1} to also satisfy the descending chain condition as a left R-module. Therefore by induction we may now conclude that R^n satisfies the descending chain condition and as use so does V. $\square$

4 Sum decomposition of A.C.C./D.C.C. Assume that a left R-module V is written as a finite sum of its submodules:

Hint: Show that extensions of A.C.C. modules are A.C.C., then induct.

$$V = \sum_{i=1}^{n} V_i.$$

Show that V is noetherian (resp. artinian) if and only if so is every V_i.

[1] When multiplying from the right, the matrix A spans R and B is fixed in S; thus, the term $T = IK + Tk$ which is K, or any k vector space.

Proof: Suppose V satisfies the ascending chain condition as a left R-module. Then given that each V_i is a submodule of V, any ascending chain of submodules of V_i is also one in V. Hence, the length of this chain must be finite in V so it must also be finite in V_i. In conclusion each V_i satisfies the ascending chain condition. The same argument follows mutatis mutandis for the descending chain condition.

Now take each V_i to satisfy the ascending chain condition. Suppose also for induction that $\sum_{i=1}^k V_i$ satisfies the ascending chain condition. First as the additive structure is an abelian group, we know $\sum_{i=1}^k V_i$ is a subgroup of V since all the submodules V_i are normal subgroups. Furthermore, given any $r \in R$,

$$r\left(\sum_{i=1}^{k} V_i)\right) = \sum_{i=1}^{k} rV_i \subseteq \sum_{i=1}^{k} V_i.$$

using the fact that each V_i is indeed a submodule. Hence $\sum_{i=1}^k V_i$ is a submodule, and moreover, so is $\sum_{i=1}^{k+1} V_i$. Finally,

$$\sum_{i=1}^{k+1} V_i / \sum_{i=1}^{k} V_i \cong V_{k+1} / \left(\sum_{i=1}^{k} V_i\right) \cap V_{k+1}.$$

Since V_{k+1} satisfies the ascending chain condition, so does

$$V_{k+1}/V_{k+1}/\left(\sum_{i=1}^{k} V_i\right) \cap V_{k+1}.$$

If we show that an extension of A.C.C. modules is A.C.C. we will have the right to conclude that V is A.C.C. by induction.

Now suppose V/W and W satisfy the A.C.C. Take a chain

$$V_0 \le V_1 \le \cdots$$

in V. This induces the chains:

$$V_0 + W/W \le V_1 + W/W \le \cdots; \qquad V_0 \cap W \le V_1 \cap W \le \cdots.$$

As both V/W and W satisfy the A.C.C. it follows both these chains stabilize. Now we use the 2nd isomorphism theorem to replace our chain in V/W with:

$$V_0/V_0 \cap W \le V_1/V_1 \cap W \le \cdots,$$

which must also stabilize in finitely many steps as it is isomorphic to the chain in V/W. Since the quotients and the intersections stabilize, the original chain stabilizes. □

Hint: Verify the the claim directly.

5 Module Bases. Let k be a field and V be a vector space over k with an infinite basis $\{e_0, e_1, \dots\}$, and $R = End_k(V)$. Let $r, s \in R$ be the elements defined by $r(e_{2n}) = e_n$, $r(e_{2n+1}) = 0$ and $s(e_{2n}) = 0$, $s(e_{2n+1}) = e_n$. Prove $\{r, s\}$ is a basis of R.

Proof: Take $\varphi, \psi \in R$ so that $\varphi r + \psi s = 0$. If we evaluate

$$\varphi(e_n) = \varphi r(e_{2n}) + \psi s(e_{2n}) = 0; \psi(e_n) = \varphi r(e_{2n+1}) + \psi s(e_{2n+1}) = 0.$$

Therefore $\varphi = 0$ and $\psi = 0$ so $\{\varphi, \psi\}$ are linearly independent. Furthermore define for every $\varphi \in R$

$$\varphi_e(e_i) = \varphi(e_{2i}); \qquad \varphi_o(e_i) = \varphi(e_{2i+1}).$$

So
$$\varphi_e(r(e_{2i})) + \varphi_o(s(e_{2i})) = \varphi_e(e_i) = \varphi(e_{2i})$$
and
$$\varphi_e(r(e_{2i+1})) + \varphi_o(s(e_{2i+1})) = \varphi_e(e_i) = \varphi(e_{2i+1}).$$
Thus, $\varphi = \varphi_e r + \varphi_o s$ so $\{r, s\}$ is a basis for R. $\square$

6 Uniqueness of Module Decomposition. – True or False? Let $V = W \oplus X$ and $V = W \oplus Y$ be decompositions of a left R-module v as direct sums of modules. Then $X = Y$.

Hint: Consider non-cyclic finite Z-modules.

Example: Consider $V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ as $\mathbb{Z}$-module. The decompositions
$$\langle(1,0)\rangle \oplus \langle(0,1)\rangle; \qquad \langle(1,0)\rangle \oplus \langle(1,1)\rangle$$
do not agree but they both are decompositions of V.

If you allow W to vary then it is worse: X need not be isomorphic to Y; consider
$$\mathbb{Z}_2 \oplus \mathbb{Z}_6 = (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_3.$$
$\square$

7 Maschke's Theorem. Let G be a finite group, F a field of characteristic p dividing $|G|$, and FG the group algebra. Consider the 1-dimensional submodule of the left regular module ${}_{FG}FG$ spanned by the element $\sum_{g\in G} g$. Show that this submodule is not a direct summand of the regular module.

Hint: Consider the augmentation ideal.

Proof: Let $x = \sum_{g\in G} g$ and take W be a complement to $\langle x\rangle$ in ${}_{FG}FG$. Hence we know
$$1 \in_{FG} FG = \langle x\rangle \oplus W$$
so $1 = \lambda x + w$ for some $\lambda \in FG$ and $w \in W$; that is, $1 - \lambda x \in W$. Therefore for any $g \in G$, $g(1 - \lambda x) \in W$ since W is an FG-module. Indeed we may take $\lambda \in F$ since $gx = x$ it is clear that
$$\lambda x = \left(\sum_{g\in G} c_g g\right)\left(\sum_{g\in G} g\right) = \left(\sum_{g\in G} c_g\right) x,$$
and each $c_g \in F$. Given that the characteristic of F divides the order of $|G|$, it must follow that $|G|\lambda = 0$ in F. Also λ commutes with g so we get
$$\sum_{g\in G} g(1-\lambda x) = \sum_{g\in G} g - g\lambda x = \sum_{g\in G}(g - \lambda g x) = \sum_{g\in G}(g - \lambda x) = x - |G|\lambda x = x.$$
However, above we resolved that this sum was in W so we must conclude that $x \in W$ which means that W does not split with $\langle x\rangle$ in ${}_{FG}FG$. Therefore $\langle x\rangle$ has no complement proving ${}_{FG}FG$ is not semi-simple. $\square$

8 Module Annihilators. – True or False?

Hint: Consider the annihilators of quotient modules.

(a) Let R be a commutative ring with ideals I, J such that $R/I \cong R/J$ (as modules), then $I = J$.

(b) Let R be any ring and I, J any two left-ideals where R/I and R/J are isomorphic as left modules, then $I = J$.

(a) **Proof:** True. Given R is a commutative ring, it follows $R \to End(R/I) : r \mapsto r(1+I)$ has kernel I, and by definition this kernel is $Ann_R(R/I)$. Hence, $I = Ann_R(R/I)$ and likewise $J = Ann_R(R/J)$. As such, if $R/I \cong R/J$ as R-modules, then we have $Ann_R(R/I) = Ann_R(R/J)$ so indeed $I = J$. $\Box$

(b) **Example:** False. With a non-commutative example we know that the annihilator of a module is always a two sided ideal, so we need only choose one sided ideals to defeat the proof above. So consider a non-commutative ring $R = M_2(F)$, with F a field. Then the left ideals

$$I = \left\{ \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \right\}, \qquad J = \left\{ \begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix} \right\},$$

give the natural projection quotients:

$$R/I \cong J, \qquad R/J \cong I.$$

There is also a natural R-module isomorphism between I and J so indeed $R/I \cong R/J$. However, $I \neq J$ visibly. $\Box$

Hint: Place the matrix for the injection from W into V in Rational Canonical Form.

9 Divisor Chains. Let $R = \mathbb{C}[[x]]$, the ring of formal power series over $\mathbb{C}$. Consider the submodule W of the free module $V = Rv_1 \oplus Rv_2$ generated by

$$u_1 = (1-x)^{-1}v_1 + (1-x^2)^{-1}v_2 \text{ and } u_2 = (1+x)^{-1}v_1 + (1+x^2)^{-1}v_2.$$

Find a basis $\{v_1', v_2'\}$ of V and elements $\delta_1 | \delta_2 \in R$ such that W is generated by $\delta_1 v_1'$ and $\delta_2 v_2'$. Describe V/W.

Example: We are asked to find unimodular matrices P and Q such that we have the following diagram:

$$\begin{tikzcd}
\mathbf{0} \arrow[r] & Ru_1 \oplus Ru_2 \arrow[r, "A"] \arrow[d, "Q"] & Rv_1 \oplus Rv_2 \arrow[r] \arrow[d, "P"] & V/W \arrow[r] \arrow[d] & \mathbf{0} \\
\mathbf{0} \arrow[r] & \delta_1 Rv_1' \oplus \delta_2 Rv_2' \arrow[r, "PAQ^{-1}"] & Rv_1' \oplus Rv_2' \arrow[r] & R/\delta_1 Rv_1' \oplus R/\delta_2 Rv_2' \arrow[r] & \mathbf{0}.
\end{tikzcd}$$

We do this by computing the Rational Canonical Form for the matrix A. We notice that if we let

$$A = \begin{bmatrix} \frac{1}{1-x} & \frac{1}{1+x} \\ \frac{1}{1-x^2} & \frac{1}{1+x^2} \end{bmatrix}$$

and consider R expressed according to v_1 and v_2, then we have $W = Span_R\{Ae_1, Ae_2\}$, with $e_1^T = (1,0)$ and $e_2^T = (0,1)$.

$$\begin{bmatrix} 1 & 0 \\ -\frac{1}{1+x} & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{1-x} & \frac{1}{1+x} \\ \frac{1}{1-x^2} & \frac{1}{1+x^2} \end{bmatrix} = \begin{bmatrix} \frac{1}{1-x} & \frac{1}{1+x} \\ 0 & \frac{-1}{(1+x)^2} + \frac{1}{1+x^2} \end{bmatrix};$$

$$\begin{bmatrix} \frac{1}{1-x} & \frac{1}{1+x} \\ 0 & \frac{-1}{(1+x)^2} + \frac{1}{1+x^2} \end{bmatrix} \begin{bmatrix} 1 & -\frac{1-x}{1+x} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{1-x} & 0 \\ 0 & \frac{-1}{(1+x)^2} + \frac{1}{1+x^2} \end{bmatrix}.$$

Since $\frac{1}{1-x}(1-x) = 1$ we know $\frac{1}{1-x}$ is a unit so it clearly divides $\frac{1}{1+x^2} - \frac{1}{(1+x)^2}$ so our matrix is in rational canonical form. Therefore the elementary divisors are $\delta_1 = \frac{1}{1-x}$ and $\delta_2 = \frac{1}{1+x^2} - \frac{1}{(1+x)^2}$. In the same way we have

$$P = \begin{bmatrix} 1 & 0 \\ -\frac{1}{1+x} & 1 \end{bmatrix}, \qquad Q^{-1} = \begin{bmatrix} 1 & -\frac{1-x}{1+x} \\ 0 & 1 \end{bmatrix}.$$

Thus to transfer V from the basis $\{v_1, v_2\}$ to $\{v_1', v_2'\}$ we simply use P.

$$\begin{bmatrix} v_1' \\ v_2' \end{bmatrix} = P \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \frac{-1}{1+x} & 1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} v_1 \\ -\frac{v_1}{1+x} + v_2 \end{bmatrix}.$$

Finally, under this new basis $\{v_1', v_2'\}$ we see

$$V/W = R/\left(\frac{1}{1-x}\right) \oplus R/\left(\frac{1}{1+x^2} - \frac{1}{(1+x)^2}\right) \cong 0 \oplus R/(x) \cong \mathbb{C}$$

using the fact that $\frac{1}{1-x}$ is a unit and that

$$\begin{aligned} \frac{1}{1+x^2} - \frac{1}{1+2x+x^2} &= \frac{1+2x+x^2}{1+2x+2x^2+2x^3+x^4} - \frac{1+x^2}{1+2x+2x^2+2x^3+x^4} \\ &= \frac{2x}{1+2x+2x^2+2x^3+x^4}. \end{aligned}$$

Since $1 + 2x + 2x^2 + 2x^3 + x^4 \in \mathbb{C}[[x]]$ it follows

$$R/\left(\frac{1}{1+x^2} - \frac{1}{(1+x)^2}\right) \cong R/(2x) \cong R/(x).$$

□

10 Composition Series – True or False? Every finitely generated module over a commutative noetherian ring has a composition series.

Hint: Consider the integers.

Example: Consider $\mathbb{Z}$. Certainly $\mathbb{Z}$ is noetherian as any ascending chain must begin with $\mathbf{0}, m\mathbb{Z}$, and from there there are only finitely many intermediate submodules. However, $\mathbb{Z}$ is not artinian as $p^i\mathbb{Z}$ is an infinite descending chain. Since $\mathbb{Z}$ is finitely generated it has a composition series if and only if it is both artinian and noetherian. Thus it has no composition series. □

11 Free Submodules – True or False? If R is a commutative ring then any submodule of a free module is free.

Hint: Consider finite rings.

Example: Consider $\mathbb{Z}_4$ over $\mathbb{Z}_4$. Certainly any ring over itself is free, and this is also a commutative ring; yet, $\mathbb{Z}_2$ is a submodule over $\mathbb{Z}_4$ but it is not isomorphic to a direct product of $\mathbb{Z}_4$ (finite means it is finitely generated as well) so $\mathbb{Z}_2$ is not free over $\mathbb{Z}_4$. □

12 Free Submodules – True or False? If R is a domain then any submodule of a free module is free.

Hint: Consider $F[x, y]$.

Example: False. Consider a field F, and its associated polynomial ring $F[x, y]$. Since F is an integral domain, so is $F[x, y]$. However, if we take the left $F[x, y]$ ideal (x, y), then we notice the relation $xy = yx$. Yet x and y are independent elements as $y \notin (x)$ and $x \notin (y)$. This means x, y cannot be a basis as there is a relation, so (x, y) is not a free $F[x, y]$ module. □

13 Free PID Modules – True or False? If R is a PID then any submodule of a finitely generated free R-module is free.

Hint: Use the canonical representation of finitely generated modules over a PID.

Proof: True. Let V be a finitely generated free R-module and W a submodule of V. From Theorem-3.7.7, and the fact that R is a PID, we know W is finitely generated and

$$W \cong R/\delta_1 \oplus \cdots \oplus R/\delta_n$$

where $d_1|\cdots|d_n$. Furthermore, as V is free, there can be no torsion in V or in any submodule W; therefore, each $d_i = 0$. So indeed, W is a finite direct product of R's so it is a free R module. $\square$

Hint: Show any two generators have relations.

14 Free Inheritance – True or False? If R is commutative and every submodule of a free R-module is free, then R is a PID.

Proof: Certainly ${}_RR$ is free so each of its submodules I is free. Suppose that I has basis $\{a_1, a_2, \dots\}$. As R is commutative it follows that $a_1a_2 = a_2a_1$ so there is a non-trivial relation between the proposed basis. Hence $a_1 = a_2 = \cdots$ is required so indeed I is generated by a single element. Since every ideal of R is a submodule, we see R is a PID. $\square$

Hint: Consider $\mathbb{Z}$.

15 PID Quotients – True or False? If R is a PID and I a proper ideal of R then R/I is a PID.

Example: Notice that what can fail is to have a quotient that is not an integral domain. For example, $\mathbb{Z}$ and $4\mathbb{Z}$ has quotient $\mathbb{Z}/4\mathbb{Z}$ which has zero-divisors; thus, while it is a principle ideal ring, it is not a domain, so it is not a PID. $\square$

Hint: Consider $\mathbb{Q}[x]$.

16 PID subrings – True or False? If R is a PID, then any subring of R is a PID.

Example: As $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is a PID; however, $\mathbb{Z}[x]$ is a subring but not a PID.

To see this consider the map:

$$\mathbf{0} \longrightarrow I = Ker\ f \longrightarrow \mathbb{Z}[x] \longrightarrow \mathbb{Z}_2 \longrightarrow \mathbf{0}$$

given by $f(p(x)) = p(0)$. This is simply an evaluation homomorphism so its properties will not be verified explicitly. Also clearly $f(1) = 1$ and $f(0) = 0$ so f is surjective so $I \neq \mathbb{Z}[x]$.

Notice also that I is simply all polynomials with even constant term, as $p(x) \in I$ whenever $f(p(x)) = p(0) = p_0 \cong 0 \pmod 2$. Suppose $I = (a(x))$ for some $a(x) \in \mathbb{Z}[x]$. Hence we have $2 \in I$ and so there must exist a $b(x) \in \mathbb{Z}[x]$ such that $2 = b(x)a(x)$ proving that $deg\ a(x) = 0$ so $a(x) = \pm 1$ or ± 2. If $a(x) = \pm 1$ then $I = \mathbb{Z}[x]$ – already seen to be false. If $a(x) = \pm 2$ then there is no $f(x)$ such that $x = f(x)a(x)$, and so we conclude that I could not be principle to begin with. $\square$

Hint: Consider $\mathbb{Z}$.

17 Polynomials over PIDs – True or False? If R is a PID then $R[x]$ is a PID.

Example: Let $R = \mathbb{Z}$. $\mathbb{Z}[x]$ is not a PID. (See Exercise-3.16.) $\square$

Hint: Consider $(x) \geq (x^2) \geq \cdots$.

18 Polynomials over Artinian Rings – True or False? If R is artinian, $R[x]$ is as well.

Example: Given any ring R, notice

$$(1) \leq (x) \leq (x^2) \leq (x^4) \leq \cdots \leq (x^{2^i}) \leq \cdots$$

so $R[x]$ is not artinian. $\square$

Hint: Consider the canonical presentation of modules over PIDs.

19 Torsion Free vs. Free – True or False? Any finitely generated torsion free module over a PID is free.

Proof: True. Since the module is finitely generated over a PID R it is equivalent to a direct sum

$$M = R/(d_1) \oplus \cdots \oplus R/(d_k).$$

However M is torsion free so each $d_i = 0$ as otherwise e_i – the canonical component generator – has non-trivial annihilator and thus has torsion. As such M is truly just a direct sum of R modules, so consequently it is a free R module. $\square$

20 Hom **over PIDs** Let R be a PID. Calculate $Hom_R(R/(a), R/(b))$.

Hint: Consider the greatest common divisor of a and b. Prove it by sending 1 in R to the map $x+(a) \mapsto \frac{b}{(a,b)}x+(b)$ in $Hom_R(R/(a), R/(b))$.

Example: The solution is $Hom_R(R/(a), R/(b)) \cong R/(a,b) \cong R/GCD(a,b)$.

Define the map $\Lambda : R \to Hom_R(R/(a), R/(b))$ by

$$\Lambda(r)(x+(a)) = r\frac{b}{GCD(a,b)}x + (b)$$

for $r, x \in R$. Since R is a PID, the greatest common divisor of a and b is defined, and furthermore, $GCD(a,b)|b$ in R. To show that Λ is well-defined take

$$x + sa \equiv x \pmod{a}.$$

From here it follows from the definition of Λ

$$\begin{aligned}
\Lambda(r)(x+sa) &\equiv r\frac{b}{GCD(a,b)}(x+sa) \\
&\equiv r\frac{b}{GCD(a,b)}x + rs\frac{ab}{GCD(a,b)} \\
&\equiv \Lambda(r)(x) + rsLCM(a,b) \\
&\equiv \Lambda(r)(x) \qquad \pmod{b}.
\end{aligned}$$

Since $\Lambda(r)$ is left translation, it is clearly an R-module homomorphism between $R/(a)$ and $R/(b)$, so Λ is well-defined.

Now we briefly demonstrate that Λ is R-linear itself:

$$\begin{aligned}
\Lambda(rs+t)(x) &\equiv (rs+t)\frac{b}{GCD(a,b)}x \\
&\equiv r\left(s\frac{b}{GCD(a,b)}x\right) + t\frac{b}{GCD(a,b)}x \\
&\equiv r\Lambda(s)(x) + \Lambda(t)(x) \\
&\equiv (r\Lambda(s) + \Lambda(t))(x) \qquad \pmod{b}.
\end{aligned}$$

Next we demonstrate that Λ is epic so we may use the first isomorphism theorem. To see this take any $g \in Hom_R(R/(a), R/(b))$. Here we know

$$0 \equiv g(0) \equiv g(a \cdot 1) \equiv ag(1) \pmod{b}.$$

However this then requires that $b|ag(1)$, and clearly we also have $a|ag(1)$, so indeed, $LCM(a,b)|ag(1)$. So there exists an $r' \in R$ such that

$$ag(1) = r'LCM(a,b) = r'\frac{ab}{GCD(a,b)} = (r'a)\frac{b}{GCD(a,b)}.$$

So if we let $r = r'a$ then we have $\Lambda(r)(1) = g(1)$ so indeed by the linearity, $\Lambda(r) = g$.

Finally we must determine the kernel of Λ to prove our assertion. Take any $r \in R$ such that $\Lambda(r)(x) \equiv 0 \pmod{b}$ for all $x \in R$. It follows then when $x = 1$ that

$$0 \equiv \Lambda(r)(1) \equiv r\frac{b}{GCD(a,b)} \pmod{b}$$

and therefore $GCD(a,b)|r$. Hence $r \in (GCD(a,b))$. And as expected, if we take

$$\Lambda(rGCD(a,b))(x) \equiv rGCD(a,b)\frac{b}{GCD(a,b)}x \equiv rbx \equiv 0 \pmod{b}.$$

So $Ker\ \Lambda = (GCD(a,b))$; thus, by the first isomorphism theorem we now can say – as R-modules:

$$R/(GCD(a,b)) \cong Hom_R(R/(a), R/(b)).$$

□

Hint: Show W contains the torsion submodule then use the canonical presentation for finitely generated modules over PIDs.

21 Pure Submodules Let R be a PID, and V and R-module. A submodule $W \leq V$ is called *pure* if $W \cap rV = rW$ for all $r \in R$. If V is a finitely generated R-module, prove that a submodule $W \leq V$ is a pure submodule if and only if W is a direct summand of V.

Proof: Given $V = W \oplus U$ take any $v \in V$ to be $v = w + u$ with $w \in W$ and $u \in U$. Certainly $rv = rw + ru$ and $rv \in rW$ if and only if $ru = rv - rw \in rW$ as clearly $rw \in rW$. Thus $ru = 0$ since $W \cap U = \mathbf{0}$. Hence $u = 0$ as this works for all $r \in R$. Therefore $v = w$ proving

$$W \cap rV = rW.$$

Now suppose that W is a pure submodule of V. Given any $r \in R$ such that $rv + W = W$, it follows $rv \in W$, so $rv \in W \cap rV = rW$. This implies $v \in W$ to begin with. So indeed, V/W is torsion-free. Hence the torsion submodule of V is contained in W. Since V is finitely generated over a PID, and $V/T(V)$ is torsion-free, it follows $V/T(V)$ is free and $W/T(V)$ remains a pure submodule of V/W. If $W/T(V)$ is a direct summand of $V/T(V)$ then by the correspondence theorem we know W is a direct summand of V. However, as $V/T(V)$ is free and $W/T(V)$ a submodule, we know there exists a suitable basis and suitable elementary divisors to present $W/T(V)$. However, the second isomorphism theorem tells us $(V/T(V))/(W/T(V)) \cong V/W$ which is torsion free, so each elementary divisor must be a unit or 0. Hence $W/T(V)$ is a direct summand of $V/T(V)$ and so W is a direct summand of V. □

Hint: Use the norm to determine which Gaussian integers are units and which are irreducible. Also recall that the Gaussian integers are a Euclidean Domain so the Euclidean algorithm applies.

22 Invariant Factors Calculate the invariant factors of the following matrices, working over $\mathbb{Z}[i]$ of Gaussian Integers:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1+i & 0 \\ 0 & 0 & 2+i \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 2i & i & 2+i \\ i-1 & 1+i & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 2+i \end{bmatrix}.$$

Example: First we recall a useful tool for working with commutative ring extensions. The norm function $N : \mathbb{Z}[i] \to \mathbb{Z} : x = a + bi \to x\overline{x} = a^2 + b^2$ sends units to units. So if the norm of a number is invertible, only then is the element invertible in $\mathbb{Z}[i]$. Also, as $N(xy) = N(x)N(y)$ it follows if $N(x)$ is irreducible then so is x. Thus using the Smith Normal Form algorithm in the first matrix we notice we need only work on the minor with top corner $2,2$. Here we add column 3 to column 2 first so that $a_{2,2} \nmid a_{2,3}$.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1+i & 0 \\ 0 & 0 & 2+i \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2+i & 0 \\ 0 & 1+i & 1+i \end{bmatrix}.$$

Using the Euclidean algorithm we find the greatest common divisor $(2+i, 1+i)$:

$$\begin{aligned} 2+i &= (1)(1+i)+1; \\ 1+i &= (1+i)(1)+0. \end{aligned}$$

As such we have 1 as the GCD and moreover

$$1 = (1)(2+i) + (-1)(1+i).$$

We also know from the proof of the Smith Normal Form algorithm that there exists $d_1, d_2 \in \mathbb{Z}[i]$ such that

$$1 = (1)d_1 + (-1)d_2; \qquad d_1 = 1, \quad d_2 = 0.$$

Finally it follows the following matrix reduces our irreducible $2+i$ by some number of irreducible factors, so in our situation it must reduce to a unit allowing us to complete the normal form by recursion on the algorithm.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2+i & 0 \\ 0 & 1+i & 1+i \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1-i \\ 0 & 2+i & 0 \end{bmatrix}.$$

Now that $a_{2,2}$ is a unit we use it to clear the second row and column.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2-i & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1-i \\ 0 & 2+i & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1-i \\ 0 & 0 & 1+3i \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1-i \\ 0 & 0 & 1+3i \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1+i \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1+3i \end{bmatrix}.$$

The invariant factors are thus $1, 1, 1+3i$. Now we move the the challenging matrix.

PENDING: redo Notice that $2+i$ is a unit and common to every term in the third column. So we clear the third column.

$$\begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} 2i & i & 2+i \\ -1+i & 1+i & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 2+i \end{bmatrix} = \begin{bmatrix} 2i & i & 0 \\ -1+i & 1+i & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 0 \end{bmatrix}.$$

Next we notice that adding row 4 to row 2 leaves the first row.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2i & i & 0 \\ -1+i & 1+i & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 0 \end{bmatrix} = \begin{bmatrix} 2i & i & 0 \\ 2i & i & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 0 \end{bmatrix}.$$

Now delete the superfluous row 2.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2i & i & 0 \\ 2i & i & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 0 \end{bmatrix} = \begin{bmatrix} 2i & i & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 0 \end{bmatrix}.$$

Now we move our units into the diagonal.

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2i & i & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2+i & 0 & 0 \\ 0 & -1 & 1+i \\ 0 & i & 2i \\ 0 & 0 & 0 \end{bmatrix}.$$

Finally we use the unit -1 to clear the second row and second column.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & i & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2+i & 0 & 0 \\ 0 & -1 & 1+i \\ 0 & i & 2i \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2+i & 0 & 0 \\ 0 & -1 & 1+i \\ 0 & 0 & -1+3i \\ 0 & 0 & 0 \end{bmatrix}.$$

$$\begin{bmatrix} 2+i & 0 & 0 \\ 0 & -1 & 1+i \\ 0 & 0 & -1+3i \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1+i \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2+i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1+3i \\ 0 & 0 & 0 \end{bmatrix}.$$

Finally we clean it up a little:

$$\begin{bmatrix} (2+i)^{-1} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2+i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1+3i \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1+3i \\ 0 & 0 & 0 \end{bmatrix}.$$

The invariant factors are $1, 1, -1+3i$ but as this unique up to units we may say it is $1, 1, -1+3i$. □

Hint: The invariant factors are $1, 2, 6$.

23 Smith Normal From Let

$$A = \begin{bmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{bmatrix}.$$

Find unimodular matrices X and Y such that XAY has the Smith Normal form: diagonal matrix with a divisor chain along the diagonal.

Example:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 4 \\ -4 & -6 & 7 \\ 6 & 6 & 15 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 2 & 4 \\ -4 & -6 & 7 \\ 6 & 6 & 15 \end{bmatrix} \begin{bmatrix} 1 & -1 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ -4 & -2 & 15 \\ 6 & 0 & 3 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 \\ -4 & -2 & 15 \\ 6 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -2 & 15 \\ 0 & 0 & 3 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & -2 & 15 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 7 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -2 & 1 \\ 0 & 0 & 3 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & -2 & 1 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 3 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 3 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 6 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 6 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{bmatrix}.$$

□

nvariant factors

24 Invariant Factors – True or False? Let R be a PID and V be a finitely generated R-module with invariant factors $\delta_1|\delta_2|\cdots|\delta_k$. Then V cannot be generated by less than k elements.

Proof: True. Take V to be generated by $\{g_1, \ldots, g_n\}$ and relators

$$f_1(g_1, \ldots, g_n) = 0, \ldots, f_k(g_1, \ldots, g_n) = 0$$

for $f_i \in R[x_1, \ldots, x_n]$. Then V is equivalently described by a $n \times k$ matrix over R Γ. This matrix Γ is equivalent to a unique Smith normal form (diagonal matrix with a divisor chain along the diagonal) Γ'. Given any other generating set, this process must produce the same Smith normal as this is an invariant of the module V. Therefore, as each time the number of invariant factors (the non-zero, non-unit divisors along the diagonal) is less than or equal to the number of generators n (they lie along the diagonal which has length less than or equal to n), it follows the number of invariant factors is the minimum number of generating elements for V. $\square$

25 Left Regular Modules – True or False? Let R be a commutative ring. Is it true that the left regular R-module is indecomposable? What if R is a PID?

Hint: For the first consider finite rings, for the second use the canonical representation of modules over a PID.

(a) **Example:** False. Consider $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. As a $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are ideal of $\mathbb{Z}_6$ they are acceptable $\mathbb{Z}_6$-modules. Moreover, they decompose $\mathbb{Z}_6$ proving it is not indecomposable. $\square$

(b) **Proof:** True. The addition of the PID condition tells us we can use the canonical presentation of finitely generated modules over a PID.

Take ${}_RR$ to be decomposed into a direct product of submodules $W_1, \ldots, W_n$. As 1 generates ${}_RR$ it follows ${}_RR$ is a finitely generated module over a PID R; therefore, there exists a generating set for ${}_RR$ such that $W_i \cong R/(d_i)$ and so that:

$${}_RR \cong R/(d_1) \oplus \cdots \oplus R/(d_n)$$

where $d_1|\cdots|d_n$ – and we allow $d_i = 0$ if free terms appear.

Now we notice that ${}_RR$ is torsion free as $sr = 0$ implies $r = 0$ or $s = 0$ as we have an integral domain. Hence we may take $d_i = 0$ for all $i = 1, \ldots, n$. However now we notice that the rank of ${}_RR$ is n, but clearly a basis for ${}_RR$ is 1. Since R is a commutative ring as a regular module it is rank invariant, so indeed $n = 1$. Therefore there is not proper decomposition of ${}_RR$ when R is a PID. $\square$

26 Matrix Equivalence – True or False? Let R be a PID and A and $n \times n$ matrix over R. Then A is invertible if and only if A is equivalent to the identity matrix.

Hint: The product of unimodular matrices is unimodular.

Proof: True. Given A is invertible it follows A^{-1} exists. Moreover, A^{-1} is also invertible so it is trivially unimodular. With this we can directly see that the equivalence

$$A^{-1}AI_n = I_n$$

where the unimodular transformation matrices are A^{-1} and I_n.

For the converse take

$$PAQ = I_n$$

with P and Q unimodular. It follows then that both P and Q are invertible so

$$A = P^{-1} I_n Q^{-1} = (QP)^{-1}.$$

As Q and P are unimodular so is their product, and so their inverse is as well; hence, A is unimodular and so invertible. □

Hint: Primary decomposition corresponds to prime factorization in $\mathbb{Z}$.

27 Invariant Factors Find the invariant factors and the primary decomposition for $\mathbb{Z}/2000\mathbb{Z}$.

Example: Given $2000 = 2^4 \cdot 5^3$ and $\mathbb{Z}/2000\mathbb{Z}$ is cyclic it follows its invariant factor is simply 2000 while its primary decomposition is simply

$$\mathbb{Z}/2000\mathbb{Z} = \mathbb{Z}/(2^4) \oplus \mathbb{Z}/(5^3).$$

□

Hint: Determine that p divides each invariant factor.

28 Primary Decomposition Let p be a prime and V be a finitely generated $\mathbb{Z}$-module with $p^a V = 0$. Suppose that $v \in V$ has order exactly p^a. Show that $V = \mathbb{Z}v \oplus W$ for some submodule $W \leq V$.

Proof: Since $\mathbb{Z}$ is a PID, and V is finitely generated it follows V decomposes as $\mathbb{Z}/d_1 \oplus \cdots \mathbb{Z}/d_k$ where $d_1|d_2|\cdots|d_k$ and d_i is a non-unit but possibly 0. Notice since $p^a V = 0$ that $p|d_i$ for all i, and $d_i \leq p^a$. Moreover, as there exists an element of order exactly p^a, it follows some $d_i = p^a$. Since v may be chosen, without loss of generality, to lie in this component of the decomposition we now see we may take as the complement of $\mathbb{Z}v$ the remaining $\mathbb{Z}/d_i$'s. □

Hint: Show first V is simply a direct sum of $\mathbb{Q}[t]$'s.

29 Endomorphisms over PIDs – True or False? Let V be a finitely generated torsion free $\mathbb{Q}[t]$- module, and $\tau \in End_{\mathbb{Q}[t]}(V)$ be surjective; then τ is injective.

Proof: True. Given this $\mathbb{Q}[t]$ is a PID we may decompose the finitely generated torsion free module V into a finite direct sum of $\mathbb{Q}[t]$. Given an endomorphism τ that is surjective we know the first isomorphism theorem applies so that $V/Ker\ \tau \cong V$. Now suppose x is a non-trivial element of the kernel of τ. It follows $\mathbb{Q}[t]x \leq Ker\ \tau$. However V is torsion free so $Ann(x) = 0$ so $\mathbb{Q}[t]x \cong \mathbb{Q}[t]$; thus,

$$Ker\ \tau \cong \mathbb{Q}[t] \oplus \cdots \oplus \mathbb{Q}[t].$$

Now we must concern ourselves with a possible "diagonal" embedding. Let $\{e_1, \dots, e_n\}$ represent a basis for V. Then if $\mathbb{Q}[t]e_i \cap Ker\ \tau \neq \mathbf{0}$ then $\mathbb{Q}[t]e_i/Ker\ \tau \cap \mathbb{Q}[t]e_i$ must be trivial or else it will have torsion; whence $e_i \in Ker\ \tau$. Therefore $Ker\ \tau$ reduces the rank of V.[2] Since the rank is finite reducing the rank cannot be surjective. Therefore the kernel must be trivial. □

Hint: Consider translation by t.

30 Endomorphisms over PIDs – True or False? Let V be a finitely generated torsion free $\mathbb{Q}[t]$-module, and $\tau \in End_{\mathbb{Q}[t]}(V)$ be injective; then τ is surjective.

Example: False. The translation by t map $\tau(x) = tx$ is always an endomorphism; however, the element t has no inverse in $\mathbb{Q}[t]$ so indeed τ is not surjective as it will not hit 1. □

Hint: Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module.

31 Torsion Free vs. Free – True or False? A (not necessarily finitely

[2] Rank of free modules over a commutative ring is invariant.

generated) torsion-free module over a PID is free.

Example: False. Given $\mathbb{Q}$ as an additive group is a $\mathbb{Z}$-module we see for any $q \in \mathbb{Q}$, $nq = 0$ implies $n = 0$ or $q = 0$ as $\mathbb{Q}$ is an integral domain and $n \in \mathbb{Q}$ whenever $n \in \mathbb{Z}$. Hence, $\mathbb{Q}$ is torsion-free.

Yet, $\mathbb{Q}$ is not a free $\mathbb{Z}$-module as it has no basis. Consider any two rational numbers a/b and c/d. Clearly

$$(cb)\frac{a}{b} + (-ad)\frac{c}{d} = ac - ac = 0$$

so $\frac{a}{b}$ and $\frac{c}{d}$ are linearly dependent. So as $\mathbb{Z} \neq \mathbb{Q}$, $\mathbb{Q}$ is not free of rank 1, and by the above it is not free of a higher rank – so $\mathbb{Q}$ is not free as a $\mathbb{Z}$-module. □

32 Rank Ordering – True or False? Let $V < W$ be a proper containment of free $\mathbb{Z}$-modules; then $rank_{\mathbb{Z}} V < rank_{\mathbb{Z}} W$.

Hint: Consider $V =_{\mathbb{Z}} \mathbb{Z}$ and its submodules.

Example: False. Consider $2\mathbb{Z} < \mathbb{Z}$. As $\mathbb{Z}$ is commutative $2\mathbb{Z}$ is an ideal and so a submodule. Moreover, $\mathbb{Z} \cong 2\mathbb{Z}$ so it is a free $\mathbb{Z}$-module. Finally, as they are isomorphic, and rank in commutative rings is invariant, it follows they both have rank 1, not one less than the other. □

33 Free Quotients – True or False? If $V \leq W$ are free $\mathbb{Z}$-modules of equal finite rank, then W/V is a finite group.

Hint: Express V in terms of the same basis as W.

Proof: True. Since both are finitely generated modules over a PID we may select a basis $\{e_1, \dots, e_n\}$ for W such that V is precisely

$$V = (\delta_1\mathbb{Z})e_1 \oplus \cdots \oplus (\delta_n\mathbb{Z})e_n$$

with $\delta_1 | \cdots | \delta_n$ and none of the δ_i's units. Furthermore, as V and W have the same rank it follows $n = rank\ V = rank\ W$, and also $d_i \neq 0$ for any i – as for then the rank of W would be less than that of V.

Now the quotient is visibly isomorphic to:

$$W/V \cong \mathbb{Z}/(\delta_1) \oplus \cdots \oplus \mathbb{Z}/(\delta_n)$$

with each δ_i a positive integer. Clearly now we know the size of the quotient to be $\delta_1 \cdots \delta_n$ which is finite. □

34 Isomorphic Quotients The $\mathbb{C}[x,y]$-modules $\mathbb{C}[x,y]/(x,y)$ and $\mathbb{C}[x,y]/(x-1, y-1)$ are isomorphic.

Hint: Recall Exercise-**??**.3.17.8 part (a) – annihilators of isomorphic quotients must agree.

Proof: False. Note from Exercise-**??**.3.17.8 part (a) we already know that two quotient modules of a commutative ring are isomorphic only when the ideals agree. So we need only show $(x,y) \neq (x-1, y-1)$.

To do this suppose $p(x,y), q(x,y) \in \mathbb{C}[x,y]$ so that

$$x = p(x,y)(x-1) + q(x,y)(y-1) = p(x,y)x - p(x,y) + q(x,y)y - q(x,y).$$

As y is not a unit nor does it divide x, it follows that $q(x,y) = 0$ is required, and $p(x,y)$ must really be a polynomial in x only. However then we allowed to take about degrees so we have

$$1 = deg\ x = deg\ p(x)(x-1)$$

which requires $p(x)$ be a constant. As 1 is not a zero-divisor it is clear that no such $p(x)$ exists so indeed $x \notin (x-1, y-1)$ so $(x,y) \neq (x-1, y-1)$ and so the two quotient modules are not isomorphic. □

35 Classification of Modules Classifying, up to isomorphism, all $\mathbb{Q}[t]$-modules V which are annihilated by $I = ((t^3-2)(t-2)^3)$ and satisfying $dim_{\mathbb{Q}} V = 5$.

Hint: Conside
contain I. This
lators of the po

Example: There are seven cyclic modules whose annihilators contain I, and thus will vanish by I, enumerated as follows:

$$V_1 := \mathbb{Q}[t]/(t-2), \quad V_2 := \mathbb{Q}[t]/((t-2)^2), \quad V_3 := \mathbb{Q}[t]/((t-2)^3),$$

$$W_1 := \mathbb{Q}[t]/((t^3-2)), \quad W_2 := \mathbb{Q}[t]/((t^3-2)(t-2)),$$

$$W_3 := \mathbb{Q}[t]/((t^3-2)(t-2)^2), \quad W_4 := \mathbb{Q}[t]/((t^3-2)(t-2)^3);$$

with dimensions over $\mathbb{Q}$ of $1, 2, 3, 3, 4, 5$, and 6 respectively. Any product of these modules will produce a modules annihilated by I, so we need only consider products that give dimension 5, which are precisely the following:

- $V_1 \oplus V_1 \oplus V_1 \oplus V_1 \oplus V_1$,
- $V_1 \oplus V_1 \oplus V_1 \oplus V_2$,
- $V_1 \oplus V_2 \oplus V_2$,
- $V_1 \oplus V_1 \oplus V_3$,
- $V_2 \oplus V_3$,
- $V_1 \oplus V_1 \oplus W_1$,
- $V_2 \oplus W_1$,
- $V_1 \oplus W_2$,
- W_3.

□

Hint: Describe the primary decomposition. This way there is an implicit ordering unlike invariant factors.

36 Abelian Groups of order $5^6 \cdot 7^5$ How many abelian groups are there of order $5^6 \cdot 7^5$?

Example: We know that in a primary decomposition the situation of one prime does not influence the other primes. Thus we can count the number of primary states of the primes 5 and 7 separately, then multiply their states to attain all possible primary decompositions which uniquely describe an abelian group of the desired order. For 5 we need only look at the number of distinct partitions on 6 – it is sufficient to insist the order of partition blocks be non-decreasing; that is, $6 = n_1 + \cdots + n_k$ and $1 \le n_1 \le \cdots \le n_k \le 6$. Thus we count.

$1,1,1,1,1,1$	$1,1,1,1,2$	$1,1,1,3$		$1,1,4$	$1,5$	$6.$
	$1,1,2,2$	$1,2,3$	$3,3$	$2,4$		
	$2,2,2$					

In total there are 11 distinct partitions. For the prime 7 we do the same only now we look at distinct partitions of 5.

$1,1,1,1,1$	$1,1,1,2$	$1,1,3$	$1,4$	5
	$1,2,2$	$2,3$		

A total of 7. Therefore the total number of distinct primary decompositions of $5^6 \cdot 7^5$ is 77; so there are 77 distinct abelian groups of order $5^6 \cdot 7^5$. □

primary decom- abelian groups.

37 Abelian Groups of order 108 Find the isomorphism class of abelian groups of order 108 having exactly 4 subgroups of order 6.

Example: Groups of the abelian variety are fully classified as $\mathbb{Z}$- modules, and thus we need only consider the possible configurations whose order is $108 = 2^2 3^3$.

For each element of order 6 we must have at least one component of order 2, and at least one component of order 3. In each group we can count the elements of order 2 as $2^i - 1$ where i is the number of $\mathbb{Z}/2^k$ modules in the primary decomposition, and likewise the elements of order 3 are counted as $3^j - 1$ where j is the number of $\mathbb{Z}/3^k$ components in the primary decomposition. Thus we can quickly count the total number of elements of order 6 in each of the possible groups as follows:

$$\begin{aligned}
\mathbb{Z}/4 \oplus \mathbb{Z}/27, &\qquad (2^1-1)(3^1-1) = 2;\\
\mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/9, &\qquad (2^1-1)(3^2-1) = 8;\\
\mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3, &\qquad (2^1-1)(3^3-1) = 26;\\
\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/27, &\qquad (2^2-1)(3^1-1) = 6;\\
\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/9, &\qquad (2^2-1)(3^2-1) = 24;\\
\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3, &\qquad (2^2-1)(3^3-1) = 68.
\end{aligned}$$

Now as the only abelian group of order 6 is $\mathbb{Z}/6$, and we know $\varphi(6) = 2$ we know each subgroup of order 6 is precisely one which contains exactly two elements of order 6. Therefore we need a group with exactly 8 elements of order 6; so our group is isomorphic to $\mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/9$. □

38 Noetherian Modules – True or False? If V is a noetherian modules over a ring, then any surjective endomorphism of V is bijective.

Hint: Consider the chain of ideals produced by the kernel of a surjection.

Proof: True. Take $f : V \twoheadrightarrow V$ to be a surjective endomorphism. We may invoke the first isomorphism theorem to state that $V/Ker\ f \cong V$. Now suppose the kernel is non-trivial. Then $f^{-1}(Ker\ f)$ is a module properly containing $Ker\ f$ as $Ker\ f$ is non-trivial. Call $K_0 = Ker\ f$ and $K_{i+1} = f^{-1}(K_i)$. This gives an ascending chain. Moreover, if $K_i = K_{i+1}$ then $f^{-1}(K_i) = K_i$ for some minimum i. Yet this requires that K_i not properly contain K_{i-1} which contradicts the minimality of i (take an element $x \in K_i \backslash K_{i-1}$, certainly $f^{-1}(x) = x + K_{i-1} \neq K_{i-1}$ as $x \notin K_{i-1}$.) So we have an infinite ascending chain which does not stabilize. So as this conflicts with the noetherian assumption it follows our insistence that $K_0 \neq \mathbf{0}$ must be false. So f is injective. □

39 Diagonal Submodules Let V and W be simple left R-modules. Suppose there exists non-zero elements $v \in V$ and $w \in W$ such that (v, w) generates a proper submodule of $V \oplus W$. Then $V \cong W$.

Hint: Consider the example $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, then use the third isomorphism theorem to prove the observation.

Proof: First we set up the appropriate diagram. Set $V' = V \oplus \mathbf{0}$ and $W' = \mathbf{0} \oplus W$ with $\mathbf{0} = \mathbf{0} \oplus \mathbf{0}$. Thus we may write $V' \cap W' = \mathbf{0}$ as they are in $V \oplus W$. Moreover, letting $U = \langle (v, w) \rangle$, we know $U \cap V' = \mathbf{0}$ or V' as V' is simple. If it is V' then as $U \neq V \oplus W$, there is a proper submodule of $V \oplus W/V' \cong W$. Yet W is simple so this cannot be. Hence $U \cap V' = \mathbf{0}$. The symmetric argument shows that $U \cap W' = \mathbf{0}$ as well. Thus we have the following lattice:

$$\begin{array}{ccccc} & & V \oplus W & & \\ & \diagup & | & \diagdown & \\ V' & & U & & W' \\ & \diagdown & | & \diagup & \\ & & \mathbf{0} & & \end{array}$$

Now we see that in fact $V \cong W$ as:

$$W \cong W'/\mathbf{0} = W'/W' \cap U \cong V \oplus W/U$$

and at the same time

$$V \cong V'/\mathbf{0} = V'/V' \cap U \cong V \oplus W/U.$$

□

Hint: Show any element avoiding V_1 and V_2 generates a subgroup of distinct from both. Then conclude such a subgroup cannot be proper.

40 Cyclic Product If V_1 and V_2 are non-isomorphic simple R-modules, then the R-module $V_1 \oplus V_2$ is cyclic.

Proof: Take any $(v, w) \in V_1 \oplus V_2 \backslash V_1 \cup V_2$ and consider the submodules $U = \langle (v, w) \rangle$. If U is a proper submodule then it cannot be V_1 or V_2 as we know (v, w) to be outside of both. As both V_1 and V_2 are simple modules, using the third isomorphism theorem we see that $V_1 \oplus V_2/V_1 \cong V_2$ and $V_1 \oplus V_2/V_2 \cong V_1$ proving U cannot contain either V_1 or V_2 and remain proper. Thus we are forced into the diagram:

$$\begin{array}{ccccc} & & V_1 \oplus V_2 & & \\ & \diagup & | & \diagdown & \\ V_1 & & U & & V_2 \\ & \diagdown & | & \diagup & \\ & & \mathbf{0} & & \end{array}$$

But this creates a problem as we know V_1 is not isomorphic to V_2; yet, this diagram tells us that:

$$V_2 \cong V_2/\mathbf{0} = V_2/V_2 \cap U \cong V_1 \oplus V_2/U$$

and at the same time

$$V_1 \cong V_1/\mathbf{0} = V_1/V_1 \cap U \cong V_1 \oplus V_2/U.$$

To avoid this contradiction we require that $U = V_1 \oplus V_2$ and therefore $V_2 \oplus V_2$ is visibly cyclic. □

Hint: Use the third isomorphism theorem to construct the lattice.

41 Simple Products If V_1 and V_2 are non-isomorphic simple R-modules then $V_1 \oplus V_2$ has exactly four submodules: $\mathbf{0} \oplus \mathbf{0}$, $V_1 \oplus \mathbf{0}$, $\mathbf{0} \oplus V_2$, $V_1 \oplus V_2$.

Proof: Since V_1 and V_2 are simple they have no non-trivial submodules, and by the third isomorphism theorem together with the correspondence theorem it follows $V_1 \oplus V_2/V_1 \cong V_2$ and $V_1 \oplus V_2/V_2 \cong V_1$ have no intermediate modules. So if there is to be a fifth submodule W it must intersect V_1 and V_2 trivially and its join with either V_1 or V_2 will be the entire module. Therefore

$$V_1 \oplus W = V_1 \oplus V_2 = W \oplus V_2.$$

Now we project along W to V_1 and along W to V_2 to see: (by the third isomorphism theorem)

$$V_1 \cong V_1/V_1 \cap W \cong V_1 \oplus W/W \cong V_1 \oplus V_2/W \cong W \oplus V_2/W \cong V_2/W \cap V_2 \cong V_2.$$

Yet we assumed to begin with that V_1 and V_2 are non-isomorphic, so we have no other modules. $\square$

42 Module Quotients – True or False? Let V be a left R-module and $V_1 \neq V_2$ be maximal submodules. Then $V/V_1 \cap V_2 \cong V/V_1 \oplus V/V_2$.

Proof: True. We set up the lattice:

$$\begin{tikzcd}[column sep=small] & V \arrow[dl, dash] \arrow[dr, dash] & \\ V_1 \arrow[dr, dash] & & V_2 \arrow[dl, dash] \\ & V_1 \cap V_2 & \end{tikzcd}$$

Since V_1 and V_2 are maximal it follows V/V_1 is simple and so by the third isomorphism theorem so is $V_2/V_1 \cap V_2$. $\square$

43 Indecomposable Modules Let R be a ring and V be an R-module. Set $E := End_R(V)$, the endomorphism ring of V.

(a) If V id the direct sum of two non-trivial R-submodules, show E contains an idempotent $e \neq 0, 1$.

(b) Suppose that all zero divisors of E lie in a proper ideal $J \in E$. Show that V is indecomposable.

Hint: Show that the sum of the two non-trivial idempotents is 1, and that both are zero-divisors.

Proof:

(a) Let $V = V_1 \oplus V_2$ and define the endomorphism

$$e_1 : V \to V : (v_1, v_2) \mapsto (v_1, 0).$$

That this is a well-defined R-linear map is clear. Moreover,

$$e_1^2(v_1, v_2) = e_1(e_1(v_1, v_2)) = e_1(v_1, 0) = (v_1, 0) = e_1(v_1, v_2)$$

proving that $e_1^2 = e_1$ so that e_1, and the associated e_2 are both non-trivial idempotents.

(b) First notice that any non-trivial ($\neq 0, 1$) idempotent is a non-trivial zero-divisor as $e^2 = e$ implies $0 = e^2 - e = e(e-1)$ and neither e nor $e - 1$ are zero. Therefore any idempotents of E are contained in this ideal J.

Now suppose V is decomposable. If $V = V_1 \oplus V_2 \oplus \cdots$ we may always take $V = V_1 \oplus W$ with $W = V_2 \oplus \cdots$. Now from part (a) we know E has two distinct idempotents e_1 and e_2. These must both be contained in J. Unfortunately,

$$(e_1+e_2)(v_1, v_2) = e_1(v_1, v_2)+e_2(v_1, v_2) = (v_1, 0)+(v_2, 0) = (v_1, v_2) = id(v_1, v_2)$$

proving that $1 = e_1 + e_2$ in E. Therefore $J = E$. Yet J was assumed to be a proper ideal so we are forced to accept that V is in fact indecomposable.

$\square$

44 Matrix Subrings – True or False? Let R be a subring of $M_n(\mathbb{Q})$ which is finitely generated as a $\mathbb{Z}$-module. Then R is free as a $\mathbb{Z}$-module.

Hint: Show R is torsion-free.

Proof: True. From the canonical representation of finitely generated modules over a PID we know that if R is torsion-free (over $\mathbb{Z}$) then it is indeed free as a $\mathbb{Z}$-module. Notice that any torsion of R is also torsion in $M_n(\mathbb{Q})$. However $\mathbb{Q}$ is torsion-free over $\mathbb{Z}$ and the action of $\mathbb{Z}$ on the matrices is component-wise multiplication so indeed there is no $\mathbb{Z}$-torsion in $M_n(\mathbb{Q})$. $\square$

Hint: Note that any endomorphism from $f : \mathbb{Q} \to \mathbb{Q}$ is completely determined by $f(1)$. Thus $End_{\mathbb{Z}}(\mathbb{Q}) = \mathbb{Q}$.

45 Schur's Lemma Converse – True or False? If V is a left R-module and $End_R(V)$ is a division ring, then V is simple.

Example: False. This demonstrates the converse of Schur's lemma cannot be obtained. Consider $\mathbb{Q}$ over $\mathbb{Z}$ as a module (as an abelian group.) We begin with a short lemma: given any integral domain R, and two maps $f, g : Q(R) \to Q(R)$ such that $f|_R = g|_R$ and both R-linear, it follows $f = g$.[3]

To prove this we resort to slight of hand:

$$nf(1/n) = f(n/n) = f(1) = g(1) = g(n/n) = ng(1/n);$$

(note $f(1) = g(1)$ because they agree on R) therefore, $f(1/n) = g(1/n)$ by the cancellation property of R. As such,

$$f(m/n) = mf(1/n) = mg(1/n) = g(m/n).$$

So $f = g$.

Now we see we can characterize any R-module endomorphism $f : Q(R) \to Q(R)$ by simply stating what $f(1)$ equals: $f(m) = mf(1)$ so $f(1)$ determines f_R and by our above lemma this is sufficient to uniquely determine f. Finally, given any $\theta \in Q(R)$, it follows $f_q(m/n) = m/n \cdot q$ is an R-module endomorphism form $Q(R)$ to $Q(R)$ so indeed $End_R(Q(R)) \cong Q(R)$ so it is a division ring (field.)

Whenever R is not finite, it follows $R \neq Q(R)$, so $Q(R)$ has R as a proper R-submodule proving $Q(R)$ is not simple. Thus Schur's lemma may not be improved in this fashion. $\square$

Hint: Notice that the given ring is itself noetherian.

46 Noetherian Modules – True or False? Every finitely generated module over $\mathbb{R}[x, y, z]/(x^2 - y^3, y^2 + z^2)$ is noetherian.

Proof: Let $R = \mathbb{R}[x, y, z]/(x^2 - y^3, y^2 + z^2)$. It is sufficient to prove that R is noetherian as any finitely generated module over a noetherian ring satisfies the ascending chain condition. [4] First not that $\mathbb{R}$ a UFD so $\mathbb{R}[x, y, z]$ is as well. So we can look at irreducible factors. If we briefly pass to $\mathbb{C}(x, y, z)$ we see we can factor these completely as follows:

$$x^2 - y^3 = (x - \sqrt{y^3})(x + \sqrt{y^3}), \qquad y^2 + z^2 = (y - iz)(y + iz).$$

However none of these factors are in $\mathbb{R}[x, y, z]$ so we now know they are irreducible and so there are no intermediate ideals proving R is in fact noetherian. $\square$

Hint: Consider $g^n - 1 = 0$.

47 Zero-Divisors in Group Algebras – True or False? If G is a finite abelian group then the group algebra $\mathbb{Q}G$ is a domain.

Example: Let $g \in G$, $g \neq 1$ and $|g| = n$, so that $g^n = 1$. Certainly then

$$(1 - g)(1 + g + g^2 + \cdots + g^{n-1}) = 1 - g^n = 1 - 1 = 0.$$

[3] When we are willing to allow ring homomorphism to send one to other numbers, then the statement can be improved to say any ring R, possibly even without a 1, and any ring homomorphisms $f, g : Q(R) \to R$ are completely determined by where they send R.

[4] From the Hilbert basis theorem this is already clear. R is a quotient of a noetherian ring so it is noetherian.

However clearly $1-g \neq 0$ and $1+g+\cdots+g^{n-1} \neq 0$ so RG has a zero-divisor. *The converse of this is an open conjecture.* $\square$

48 Commutative Semi-simple Rings – True or False? A commutative ring is left semi-simple if and only if it is isomorphic to a direct sum of finitely many fields.

Hint: Show matrices commute only if they have dimension 1.

Proof: True. A semi-simple ring is isomorphic to a finite product of matrix rings over division rings by the Wedderburn-Artin theorem. First of all, as the division ring is embedded in every matrix ring over the division ring, it follows for our ring to be commutative that each of the prescribed division rings be commutative. Furthermore, any non-trivial matrix ring over a field remains non-commutative as it has elements of the form:

$$A = \begin{pmatrix} 0 & 1 & \cdots \\ 1 & 0 & \\ \vdots & & \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & \cdots \\ 0 & 0 & \\ \vdots & & \end{pmatrix}$$

which yield:

$$AB = \begin{pmatrix} 0 & 0 & \cdots \\ 1 & 0 & \\ \vdots & & \end{pmatrix}, \qquad BA = \begin{pmatrix} 0 & 1 & \cdots \\ 0 & 0 & \\ \vdots & & \end{pmatrix},$$

which clearly are not equal. Therefore the dimension of each matrix must be 1×1 and so in fact the ring is simply a finite product of fields. $\square$

49 Idempotents and $J(R)$ Prove that $J(R)$ contains no non-zero idempotent.

Hint: Show any non-trivial $(\neq 0, 1)$ idempotent is a zero-divisor.

Proof: True. We use the characterization of the Jacobson radical as the set of all $x \in R$ such that for any $r \in R$, $1-rx$ is left invertible. Given any non-trivial idempotent $e \neq 0, 1$, we quickly see e is a zero-divisor (on the left and right) as $0 = e - e^2 = e(1-e) = (1-e)e$. Therefore $1-e$ is not invertible on the left or right so it is not in the Jacobson radical. Furthermore, $1 \notin J(R)$ as 1 is not in any maximal ideal. So the only idempotent in $J(R)$ is 0. $\square$

50 Nilpotent Ideal – True or False? In a ring R the set of nilpotent elements is an ideal.

Hint: Consider non-commutative rings.

Example: False. If R is commutative then it is true and the ideal is precisely the nil-radical $\sqrt{\mathbf{0}}$. However if we take the non-commutative ring $M_2(\mathbb{Q})$ we quickly find two nilpotent elements:

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

where $A^2 = 0$ and $B^2 = 0$; yet, $A + B$ a unit (it is a permutation matrix). Thus if A and B are in a ideal in $M_2(\mathbb{Q})$ then this ideal is the entire ring. As the identity is not nilpotent it is clear such an ideal is not simply composed of nilpotent elements. $\square$

51 Nilpotency in Semi-simple Rings – True or False? If R is a commutative semi-simple ring and $r \in R$ with $r^2 = 0$ then $r = 0$.

Hint: The Jacobson radical of a commutative ring contains all nilpotent elements.

Proof: True. Given R is semi-simple it follows $J(R) = 0$. Furthermore, as R is commutative it contains all nilpotent elements; so $r \in J(R) = \mathbf{0}$. Without further question, $r = 0$. $\square$

Hint: Use Wedderburn-Artin.

52 Semi-simple Rings of order 4 R is a semi-simple finite ring of order 4. What must R be?

Example: Two possibilities arise immediately: the field of order 4 $\mathbb{F}_4$ and the product of the field of order 2, $\mathbb{F}_2 \oplus \mathbb{F}_2$.

Now we prove these. Given R is semi-simple, by the Wedderburn-Artin theorem it is a product of matrix rings over division rings. As these must be finite, so must the division ring. Indeed by the little theorem of Wedderburn, every finite division ring is a field. The smallest non-trivial matrix ring $M_2(\mathbb{F}_2)$ already has 16 elements, so in fact our ring a product of fields. Therefore it can only be $\mathbb{F}_2 \oplus \mathbb{F}_2$ or $\mathbb{F}_4$. $\square$

Hint: Consider a local ring.

53 Jacobson Radical – True or False? For every left noetherian ring R, the Jacobson radical $J(R)$ is the largest nilpotent ideal of R.

Example: False. When R is artinian this is true. However when we take a noetherian non-artinian local ring such as $\mathbb{C}[[x]]$ we see we get $J(\mathbb{C}[[x]]) = (x)$ – the unique maximal ideal (left/right do not matter as we have a commutative ring).[5] However (x) is not a nilpotent ideal. Notice $(x)^n = (x^n) \neq \mathbf{0}$ for any $n \in \mathbb{Z}^+$. $\square$

Hint: Consider the integers.

54 Semi-simple Rings – True or False? If R is a noetherian commutative ring then $R/J(R)$ is a semi-simple ring (i.e.: every R-module is semi-simple).

Example: False. Let $R = \mathbb{Z}$. $\mathbb{Z}$ is noetherian and any chain of ideals beginning with $\mathbf{0}$ must next go to $m\mathbb{Z}$ for some m. From here there are only finitely many ideals until $\mathbb{Z}$ is reached. Also, the maximal ideal of $\mathbb{Z}$ are $p\mathbb{Z}$ where p is prime. So the intersection is the set of all integers which every prime divides; so $J(R) = \mathbf{0}$. Hence $R/J(R) \cong R$. Yet $\mathbb{Z}$ is not semi-simple as it is not artinian: evidenced by $(1) > (2) > (4) > (8) > \cdots$. $\square$

Hint: Maximal ideal in $\mathbb{Z}$ correspond to primes.

55 Jacobson Radical of $\mathbb{Z}/m$ Calculate the Jacobson radical of the ring $\mathbb{Z}/m\mathbb{Z}$.

Example: Since prime ideals are maximal in a PID, we have $p\mathbb{Z}$ as the maximal ideals of $\mathbb{Z}$ where p is prime. Thus when we consider $\mathbb{Z}/m\mathbb{Z}$, the maximal ideals are $p\mathbb{Z}/m\mathbb{Z}$ where $p|m$ (if $(p, m) = 1$ then $m\mathbb{Z}$ is not a subring of $p\mathbb{Z}$, so it is not included in the quotient lattice.) Now their intersection follows their intersection in $\mathbb{Z}$: $p\mathbb{Z} \cap q\mathbb{Q} = [p, q]\mathbb{Z}$, where $[p, q]$ is the least common multiple of p and q; hence, the intersection of maximal ideals in $\mathbb{Z}/m\mathbb{Z}$ is:

$$[p_1, \ldots, p_n]\mathbb{Z}/m\mathbb{Z}, \qquad p|m.$$

A final cosmetic step is to observe that $k\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/(m/k)\mathbb{Z}$ where $k|m$ (as otherwise the quotient is not defined.) So we may write:

$$J(\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/GCD_{p|m}\left(\frac{m}{p}\right)\mathbb{Z}.$$

$\square$

Hint:

56 Idempotents and Jacobson Radicals Let $e \in R$ be a non-zero idem-

[5] $\mathbb{C}[[x]]$ is noetherian by the Hilbert basis theorem, and not artinian by the obvious descending chain $(x) > (x^2) > (x^3) > \cdots$.

potent. Then eRe is a ring and $J(eRe) = J(R) \cap eRe$.

Proof: Given $a, b \in R$, notice $eae + ebe = e(a+b)e \in eRe$. Also notice

$$eae + e(-a)e = e(a-a)e = e0e = 0$$

so $e(-a)e = -eae$ and thus R contains inverses, and clearly also 0 so it is non-empty and thus a subgroup of R under addition. Also notice $(eae)(ebe) = eaeebe = e(aeb)e$ which is in R and so eRe is closed under multiplication; moreover, the multiplication is associative since it is also in R. For unity we take e, and notice that indeed:

$$(eae)(e) = eae = e(eae).$$

Hence, eRe is a unital ring.[6]

Now consider a simple left R-module V. We may take eV and all the properties for eRe-modules hold, with the only interesting feature being the unital nature:

$$e(ev) = eev = ev.$$

So we have eV as an eRe-module, although possibly trivial. Thus the annihilators of simple eRe-modules in eRe are a subcollection of the annihilators of simple R-modules, intersected with eRe. So $J(eRe) \subseteq J(R) \cap eRe$. **PENDING:** reverse inclusion $\square$

57 Jacobson Radical of Matrices Let R be a ring. Show that $J(M_n(R)) = M_n(J(R))$. **Hint**:

Remark 3.0.9 *The following proof is a farce. Our recent examples over $\mathbb{Z}$ show that left ideals such as:*

$$M_2(\mathbb{Z}) \cdot \begin{pmatrix} 1 & 5 \\ 0 & 7 \end{pmatrix}.$$

are maximal and yet clearly not contained in any of the proposed maximal matrices in the proof. These may in fact not be maximal, but certainly are not sufficient.

Proof: Let $\{J_i \ : \ i \in I\}$ be the maximal left ideals of R. First we claim the maximal left ideal of $M_n(R)$ are the sets

$$m_k(J_i) = \{(a_{i,j} \in M_n(R) \ : \ a_{i,k} \in J_i\}$$

for all $i \in I$ and all $k = 1, \dots, n$. Since each J_i is closed to sums and absorbs products on the left, it follows each $m_k(J_i)$ is a left ideal of $M_n(R)$. Furthermore, as each J_i is maximal in R, we cannot adjoin any other matrices without forcing the k-th column to contain all elements of R, and thus obtain $M_n(R)$; hence, each $m_k(J_i)$ is maximal in $M_n(R)$.

Now suppose M is a maximal left ideal of $M_n(R)$. It follows then we may express $M = (I_{i,j})$ where $I_{i,j}$ are each left ideals of R. Moreover, as we can multiply on the left by permutation matrices – an action that can resort rows – we must have each column with the same ideal; that is, $I_{i,k} = I_{j,k}$ for all i, j and k. Now to be proper, we must have some column ideal $I_{i,k}$ be a proper ideal in R. To remain maximal we require that only one column have this, and that this column's ideal be maximal in R. Hence the maximal left ideal in $M_n(R)$ are in fact exactly all $m_k(J_i)$.

[6] Even when R itself it not unital we have this situation; however, when R has unity 1, then $e = e1e$ as expected.

Now intersect these maximal ideals and we see as i ranges that each column space must have entries over the intersection of all maximal left ideals – $J(R)$. Furthermore, letting k range we see each column must be over $J(R)$, and so the matrices themselves are exactly those of $M_n(J(R))$. $\square$

Hint: Use Nakayama's Lemma.

58 Nakayama's Lemma Let V be a finitely generated left R-module, and $\pi : V \to V/J(R)V$ be the projection. If $\pi(v_1), \ldots, \pi(v_n)$ generate $V/J(R)V$, then $v_1, \ldots, v_n$ generate V.

Proof: Let W be the span of $v_1, \ldots, v_n$ and as required assume $W + J(R)V = V$ since $\pi(v_1), \ldots, \pi(v_n)$ generates $V/J(R)V$ (this is not assuming what is to be proved, it is simply writing the same details as cosets.) Thus by Nakayama's Lemma we have $W = V$, so indeed the vectors span V. $\square$

Hint: Use the result of Exercise-3.56 to determine the internal direct product.

59 Jacobson Radical – True or False? $J(R_1 \oplus \cdots \oplus R_n) = J(R_1) \oplus \cdots \oplus J(R_n)$.

Proof: True. We saw in Exercise-3.56 that given a non-trivial idempotent e, eRe formed a ring and furthermore $J(eRe) = J(R) \cap eRe$. Now take the idempotents $e_1 = (1, 0, \cdots, 0)$ through $e_n = (0, \ldots, 0, 1)$ in $R = R_1 \oplus \cdots \oplus R_n$. It follows that $e_iRe_i \cong R_i$. Also,

$$J(R) \cap e_iRe_i = J(e_iRe_i) \cong J(R_i).$$

As such we see that

$$J(e_iRe_i) \cap J(e_jRe_j) = \mathbf{0}$$

whenever $i \neq j$. Also clearly

$$J(R) = J(e_1Re_1) + \cdots + J(e_nRe_n).$$

Therefore we have the ingredients for an internal direct product:

$$\begin{aligned} J(R_1) \oplus \cdots \oplus J(R_n) &\cong J(e_1Re_1) \oplus \cdots \oplus J(e_nRe_n) \\ &= J(e_1Re_1 \oplus \cdots \oplus e_nRe_n) \\ &= J(R_1 \oplus \cdots \oplus R_n). \end{aligned}$$

$\square$

Hint: Express R in its primary decomposition.

60 Jacobson Radicals of PIDs Let F be a field and $R = F[x]/I$ where I is the ideal of $F[x]$ generated by $x^2 + 2x + 1$. What is the Jacobson radical of R?

Example: Notice first that $x^2 + 2x + 1 = (x + 1)^2$ and $x + 1$ is irreducible. As $F[x]$ is a PID it follows irreducible elements generate maximal ideals. Since we have a commutative ring we care only about full ideals, not left. Furthermore, $I = ((x + 1)^2)$ is $(x + 1)$-primary so our quotient ring has precisely one maximal ideal, namely $(x + 1)/((x + 1)^2)$. Therefore the Jacobson Radical is $(x + 1)/((x + 1)^2)$. $\square$

Hint: Use Nakayama's Lemma.

61 Nakayama's Lemma Prove the following generalization of Nakayama's Lemma. If R is an arbitrary ring, I a two-sided ideal of R contained in the Jacobson Radical of R, and V a left finitely generated R-module such that $IV = V$, then $V = 0$.

Proof: Since I is contained in $J(R)$, it follows $J(R)V \geq IV = V$, and so $J(R)V = V$. However Nakayama's lemma tells us that $0 + J(R)V = V$ implies $V = 0$, so we are done. $\square$

ur's Lemma

62 Schur's Lemma – True or False? If V is an irreducible R-module, the center of $End_R(V)$ is a field.

Proof: True. By Schur's Lemma we recognize the $End_R(V)$ is a division ring. The center of a division ring is a commutative division ring and so it is a field. □

63 Semi-simple Rings Say what you can about an artinian ring containing no non-zero nilpotent elements.

Hint: Consider nilpotent ideals first.

Example: Given any nilpotent ideal, all its elements are nilpotent. Thus, each nilpotent ideal is trivial. Moreover, the Jacobson radical is the maximal nilpotent ideal since our ring is artinian; so it must, therefore, be trivial. As our ring is artinian and has trivial Jacobson radical, we now see it is a semi-simple ring.

As any semi-simple ring is artinian and has trivial Jacobson radical, (and consequently no non-zero nilpotent elements) this statement cannot be improved. □

64 Division Rings – True or False? If R is a left artinian ring containing no zero-divisors, then R is a division ring.

Hint: Use the Wedderburn-Artin theorem.

Proof: True. As R has no zero-divisors it has no nilpotent elements, and thus also no nilpotent ideals. Hence the Jacobson radical is trivial as in an artinian ring it is always nilpotent; therefore, R is semi-simple artinian. Making use of the Wedderburn-Artin theorem we now see

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k).$$

However if any $n_i > 1$ then there are zero-divisors, for example:

$$A = \begin{bmatrix} \cdots & 0 & 1 \\ & & 0 \\ & & \vdots \end{bmatrix}$$

is nilpotent so it is a zero-divisor. Hence

$$R = D_1 \oplus \cdots \oplus D_k.$$

Yet even this is a problem as we have idempotents (for example $(1, 0, \ldots, 0)$) which are not 0 or 1, and such elements are always zero-divisors.[7] We are left with the conclusion

$$R = D_1$$

where D_1 is a division ring. □

65 Division Algebras – True or False? Let F be a field. A finite dimensional F-algebra without zero-divisors is a division algebra.

Hint: Show A is left artinian then use Exercise-3.64.

Proof: True. Let A be a finite dimensional F-algebra with no zero-divisors. Given any left ideal I in A, it follows I is an F-subspace of ${}_FA$. Take a chain of descending left ideals $I_0 \geq I_1 \geq \cdots$ in A. It follows with it we get

$$dim_F A \geq dim_F I_0 \geq dim_F I_1 \geq \cdots .$$

Yet F is a field so if $dim_F I_i = dim_F I_{i+1}$ then $I_i = I_{i+1}$. As the total dimension of A as an F-vector space is finite it follows the descending chain stabilizes in

[7] $e(1-e) = 0$, $e \neq 0$, $1 - e \neq 0$.

finitely many steps; hence, A is left-artinian. As A has no zero-divisors, as we saw in Exercise-3.64, it is semi-simple and consequently also a division ring, our in our case a division algebra. □

Hint: Every simple artinian ring is isomorphic to a ring of matrices over a division ring.

66 Simple Artinian Rings – True or False? If a ring R is simple artinian then the ring of all 2×2 matrices over R is simple artinian.

Proof: True. As the Jacobson radical is a two-sided ideal, in R it must be trivial. As R is also artinian it follows it is in fact semi-simple artinian. So by the Wedderburn-Artin theorem we know

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k).$$

Yet unless $k = 1$, there are two sided ideals in this presentation (we see this by the projection map π_1 which has as its kernel the ideal $M_{n_2}(D_2) \oplus \cdots \oplus M_{n_k}(D_k)$.) Therefore $R = M_n(D)$. There is an obvious isomorphism between $M_2(M_n(D))$ and $M_{2n}(D)$; therefore, it is simple artinian as matrix rings over division rings are always simple artinian. □

Hint: Show $FG/J(FG)$ is semi-simple artinian.

67 Group Algebras Let G be a finite group and F be an algebraically closed field of characteristic p. Prove the following:

(i) Up to isomorphism, that there are only finitely many irreducible FG-modules $L_1, \ldots, L_k$.

(ii) Let $d_i = dim\ L_i$, $1 \leq i \leq k$. Then $\sum_{i=1}^k d_i^2 \leq |G|$, and the equality holds if and only if $p \nmid |G|$.

(iii) Is it true that the inequality $\sum_{i=1}^k d_i^2 \leq |G|$ holds even if F is not algebraically closed?

Proof: Since any field F is commutative, left ideals are in fact ideals and so F has no proper left ideals. Hence F is trivially artinian. Since G is finite, and FG is a finite dimensional F vector space (hence $FG \cong F \times \cdots F$ over F) it follows FG is artinian. Consider the Jacobson radical $J = J(FG)$, [which is trivial when $char\ F$ does not divides the order of G – Maschke's Theorem.]

Study FG/J. As J is an ideal of FG, this quotient is a well-defined ring. Moreover, as quotients of artinian rings are artinian, and $J(FG/J) = 0$, we now see FG/J is semi-simple artinian. We now may consider any simple left FG/J module V. Since J annihilates all simple FG modules, we may inflate V to and FG-module, and for the same reason we may go back. Thus there is a one to one correspondence between the simple FG-modules and the simple FG/J-modules.

We may now answer the first problem: FG/J is semi-simple artinian, so it has finitely many irreducibles – make use here of the Wedderburn-Artin representation of semi-simple rings.

The second result follows from that fact that our modules are inflated to FG-modules. Clearly from the Wedderburn-Artin theorem, the modules over FG/J have the property that $\sum_{i=1}^k d_i^2 = |G|$. However, over a larger ring, the dimensions are possibly less. Using Maschke's theorem, the equality holds whenever p does not divide the order of G.

Finally for the third question is false. For example, given C_3, we may use $\mathbb{Q}$ and study $\mathbb{Q}C_3$. For notational convenience let C_3 be generated by a primitive 3rd root of unit ω.

It follows $e = 1 + \omega + \omega^2$ is an idempotent. Its associated principal ideal $\mathbb{Q}C_3e = \mathbb{Q}e$ is simple as it is isomorphic to $\mathbb{Q}$. We also immediately see $\mathbb{Q}C_3 =$

$\mathbb{Q}e \oplus \mathbb{Q}C_3(1-e)$. We also notice that $\mathbb{Q}C_3(1-e) = \mathbb{Q}(\omega)$. Hence as it is a field it too is simple. So we have our simple decomposition:

$$\mathbb{Q}C_3 = \mathbb{Q}(1+\omega+\omega^2) \oplus \mathbb{Q}(\omega)$$

and as $dim_{\mathbb{Q}}\mathbb{Q}(\omega) = 2$ and clearly $1^1 + 2^2 > 3$. □

68 Group Algebras Let C_n be the cyclic group of order n. Decompose the group algebra $\mathbb{C}C_n$ as a direct sum of simple ideals. Do the same for $\mathbb{Q}C_n$.

Hint:

Example: Let F be either $\mathbb{Q}$ or $\mathbb{C}$. Let $C_n = \langle \omega \rangle$ where for convenience $\omega \in \mathbb{C}$ is a primitive n-th root of unity when $F = \mathbb{Q}$ and simply an abstract generator outside of $\mathbb{C}$ when $F = \mathbb{C}$. The element $e = 1 + \omega + \cdots + \omega^{n-1}$ lies in FC_n and furthermore, the left ideal $L_1 = FC_n e = Fe$ so $dim_F L_1 = 1$. This means L_1 is an irreducible FC_n-module as any smaller module would have dimension 0.

It also follows that $e^2 = e$ so we see that ${}_{FC_n}FC_n = FC_n e \oplus FC_n(1-e)$. Now we need to decompose $FC_n(1-e)$. Notice what elements look like here:

$$\sum_{i=0}^{n-1} a_i\omega^i \cdot (-\omega - \omega^2 - \cdots - \omega^{n-1}) = -\sum_{k=1}^{n-1}\sum_{i=0}^{n-1} a_i\omega^{i+k}.$$

So let $a_0 = -1$ and $a_i = 0$ for all $i > 0$. Then the result is simply ω. Hence, $F(\omega) \leq FC_n(1-e)$.

One final general property is to note that each left ideal of FC_n is an F-vector space. Add to this the fact that FC_n is semi-simple artinian by Maschke's theorem and it is commutative so we know it is a product of fields. Hence the decomposition must have the following property:

$$FC_n \cong F_1 \oplus \cdots \oplus F_k$$

where $dim_F F_1 + \cdots + dim_F F_k = dim_F FG = |G|$.

Now we make use of the specific fields.

When $F = \mathbb{Q}$ it follows $F(\omega) = \mathbb{Q}(\omega)$, and $2 = dim_{\mathbb{Q}}\mathbb{Q}(\omega) \leq dim_{\mathbb{Q}}\mathbb{Q}C_n \leq 2$. Therefore $\mathbb{Q}C_n(1-e) = \mathbb{Q}(\omega)$ and as such it is a field so we have satisfied the Wedderburn-Artin claim and as such we know $L_2 = \mathbb{Q}C_n(1-e)$ to be irreducible and finally that

$$\mathbb{Q}C_n = \mathbb{Q}e \oplus \mathbb{Q}C_n(1-e) \cong \mathbb{Q} \oplus \mathbb{Q}(\omega).$$

When $F = \mathbb{C}$ the result is little different. The fact that all finite dimension field extensions of $\mathbb{C}$ are of degree 1 forces us to admit $dim_{\mathbb{C}} F_i = 1$ for all i and so there are L_2 through L_n all isomorphic to $\mathbb{C}$. Now we must find their generators by decomposing $\mathbb{C}C_n(1-e)$. □

69 Commutative Algebras – True or False? Let A be a finite dimensional commutative algebra over an algebraically closed field F. Then all simple A-modules are 1 dimensional over F.

Hint: Use The Jacobson Density Theorem together with Schur's Lemma.

Proof: True. The proof is a trail of falling dominoes. Let V be a simple A-module. From Schur's lemma it follows $End_A(V)$ is the field F, since F is algebraically closed, V is simple, and A is an F-algebra. Now as A is finite dimensional over F, we know any quotient by a left ideal is also finite dimensional, and in particular our simple module V, which is isomorphic to one such quotient, must be finite dimensional as an F vector space.

Now we consider $End_F(V)$ which is all F-linear maps from V to V and hence completely determined by a finite basis $\{e_1, \ldots, e_n\}$. However, V is simple and each of its two submodules has each other as a complement so V is semi-simple. Hence we may invoke the Jacobson Density Theorem to infer that to any $f \in End_F(V)$ there exists an $r \in A$ such that $f(e_i) = re_i$. Since F is central in A it follows:

$$f(\vec{x}) = f(a_1 e_1 + \cdots a_n e_n) = ra_1 e_1 + \cdots ra_n e_n = r\vec{x}$$

where $a_i \in F$, and $\vec{x} \in V$ as an F vector space. Therefore f is completely characterized by left translation, and as any r produces a viable F-linear endomorphism of V, we now see there exists a surjective ring epimorphism form A onto $End_F(V)$.[8]

Finally we observe the $End_F(V)$, being simply linear transformations of a finite dimensional vector space, must coincide with $M_n(F)$. However this requires A map surjectively as a ring onto $M_n(F)$. Since A is given as a commutative ring, it follows $M_n(F)$ must also be commutative, which requires $n = 1$. Thus V is 1-dimensional over F. □

Hint: Consider $\mathbb{Q}C_4$.

70 Commutative Algebras – True or False? Let A be a finite dimensional commutative algebra over a field F. Then all simple A-modules are 1 dimensional over F.

Example: False. Consider $\mathbb{Q}C_4$. In Exercise-3.68 we saw that

$$\mathbb{Q}C_4 \cong \mathbb{Q} \oplus \mathbb{Q}(\omega)$$

where ω is a primitive fourth root of unity. As $dim_{\mathbb{Q}}\mathbb{Q}(\omega) = 3$ we see it is not of dimension 1. □

Hint: Use the Jacobson Density Theorem.

71 Simple Modules over Algebras Let A be a finite dimensional algebra over an algebraically closed field F, and V be simple A-module.

(i) Show that V is finite dimensional.

(ii) Let $\{v_1, \ldots, v_n\}$ be a basis of V, and $\pi(b)$ be a matrix of a linear transformation $V \to V$, $v \mapsto bv$ with respect to this basis. Show that for any matrix $B \in M_n(F)$ there exists $b \in B$ with $B = \pi(b)$.

(iii) Show that (ii) may fail if F is not algebraically closed.

Proof: Certainly V is a quotient of A, so it is an F vector space. Moreover, V has finite dimension over F as A has finite dimension, and quotients of vector spaces have dimensions less than or equal to the original. Now assume $v_1, \ldots, v_n$ is a basis of V over F. As Schur's lemma applies, we know the endomorphisms of V over A are simply F. Moreover, now the Jacobson Density Theorem applies, since simple modules are semi-simple, so we get that $End_F(V)$ is characterized completely by scalar transformations given a finite number of vectors. Yet we have a finite F dimensional space so we have indeed all our transforms are scalar. Thus, as $End_F(V) = M_n(F)$ we see to every matrix B of $M_n(F)$ there exists a scalar b such that $B = \pi(b)$. □

Example: For the counter-example let $F = \mathbb{R}$ and consider $V =_{\mathbb{C}} \mathbb{C}$ as an $\mathbb{R}$-algebra. As $dim_{\mathbb{R}}\mathbb{C} = 2$ we see that indeed $\mathbb{C}$ is a finite dimensional algebra

[8]

$$\begin{aligned} f_r(s\vec{x} + \vec{y}) &= rs\vec{x} + r\vec{y} = sf_r(\vec{x}) + f_r(\vec{y}); \\ (f_r + f_s)(\vec{x}) &= r\vec{x} + s\vec{x} = (r+s)\vec{x} = f_{r+s}(\vec{x}), \\ f_r \circ f_s(\vec{x}) &= rs\vec{x} = f_{rs}(\vec{x}). \end{aligned}$$

over $\mathbb{R}$. Clearly V is a simple $\mathbb{C}$-module as $\mathbb{C}$ has no proper ideals. The matrix corresponding to complex conjugation, namely

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

is not scalar. □

72 Finite Rings A finite ring with no nilpotent elements is a direct product of fields.

Hint: Use the Wedderburn-Artin theorem.

Proof: Given a finite ring R, it can have only finitely many subsets and so also only finitely many left ideals. Hence it is left artinian. As such, the Jacobson radical is a nilpotent ideal, and so every element of $J(R)$ is nilpotent. Since we also assume R has no nilpotent elements it is clear that $J(R) = \mathbf{0}$. Thus R is semi-simple artinian. By the theorem of Wedderburn-Artin we know

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k).$$

Yet as seen many times before, every matrix ring with $n > 1$ has nilpotent elements so each $n_i = 1$. Moreover by the little theorem of Wedderburn we know each finite division ring is a field, so we are left with the conclusion that R is a direct product of fields. □

73 Finite Simple Rings Describe the finite simple rings.

Hint: Use Wedderburn-Artin and the little Wedderburn theorem.

Example: Every finite ring is trivially left artinian. Moreover, as R is simple, it has only one maximal two-sided ideal – the trivial ideal – so $J(R) = 0$ as it is a two-sided ideal and must be contained in a maximal ideal. Thus R is left semi-simple. Therefore R is simple and semi-simple then by Theorem-3.11.13 we know $R \cong M_n(D)$ for some division ring D. Furthermore, D is embedded in $M_n(D)$ which must be finite, so it is a finite division ring and hence by the little Wedderburn theorem, D is a field. Finally we can say $R \cong M_n(F)$ for some finite field F.

Now, given any finite field $\mathbb{F}_{p^k}$, we know from Thm-3.11.13 that $M_n(\mathbb{F}_{p^k})$ is simple. Moreover, for each n it is also finite, so the description cannot be improved as each $M_n(\mathbb{F}_{p^k})$ is a viable simple finite ring.

It may be of interest to note that each finite simple ring has order p^{kn^2} and for each p^m there are exactly as many simple rings as there are ways to write $m = kn^2$. In particular, there is only a unique simple ring (the field) of order p^q where p and q are prime. □

74 Complex Algebra Dimensions – True or False? If A is a finite dimensional simple algebra over $\mathbb{C}$, then $dim_{\mathbb{C}}\ A$ is a perfect square.

Hint: Use the Wedderburn-Artin theorem.

Proof: True. Since A is a finite dimensional $\mathbb{C}$-algebra, it follows any descending chain of left ideals must have distinct dimensions over $\mathbb{C}$ for each step. Being finite dimensional over all, all such chains must stabilize in finitely many steps. Thus A is left artinian. Moreover, A is simple so its Jacobson radical is trivial as $J(A)$ is a two-sided ideal. Therefore A is semi-simple artinian and so we invoke the Wedderburn-Artin Theorem to state:

$$A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

for division rings D_i.

Finally we have proper two-sided ideals $M_{n_i}(D_i)$ if $k \neq 1$. So since A is simple we require $k = 1$. Thus indeed

$$A \cong M_n(D).$$

As such, $dim_{\mathbb{C}}\ A = dim_{\mathbb{C}}\ M_n(D) = (dim_{\mathbb{C}}\ D)^2$ so the dimension is a perfect square.

One final problem is if $n = 1$ and so $dim_{\mathbb{C}}\ A = dim_{\mathbb{C}}\ D$. However such a division ring is a division $\mathbb{C}$-algebra and is also finite dimensional. We will show this requires $\mathbb{C} = D$ since $\mathbb{C}$ is algebraically closed.

Given any finite dimensional field of extension is algebraic, there are only trivial finite dimensional field extensions of $\mathbb{C}$. Also, $\mathbb{C}$ is in the center of D. Now take $a \in D$. It follows for any $x \in \mathbb{C}$ that $ax = xa$ so indeed $\mathbb{C}(a)$ is a field. Yet $\mathbb{C}(a)/\mathbb{C}$ is a finite field extension and so $\mathbb{C}(a) = \mathbb{C}$. In conclusion $D = \mathbb{C}$. $\square$

Hint: Use the correspondence theorem on some maximal left ideal properly containing J.

75 Division Rings Let R be a ring and J be its Jacobson Radical. Then R/J is a division ring if and only if R has a unique maximal left ideal.

Lemma 3.0.10 *A ring R with identity $1 \neq 0$ is a division ring if and only if R has no proper left ideals.*

Proof: Consider R, a unital ring. When R is a division ring and I a left ideal of R, I must absorb product. But for all $r \in I$, if $r \neq 0$ then there exists a left inverse r' such that $r'r = 1$. Therefore when I is nonzero it is the entire ring. So R has no proper left ideals.

Consider R to be a unital ring with no proper left ideals. Given any nonzero element a in R, which must exists since $1 \neq 0$, then Ra is a left ideal. Left ideals may not be proper so Ra is $\mathbf{0}$ or R. The unity of R allows $a \in Ra$ where $a \neq 0$ so $Ra = R$. Thus $1 \in Ra$ so there exists an a' such that $1 = a'a$, so a is left invertible.

Having shown $Ra = R$ for all nonzero a in R take a and b to be non-zero elements in R and suppose they are zero-divisors so that $ab = 0$. Thus it would follow that $0 = R0 = Rab = (Ra)b = Rb = R$ but $1 \neq 0$, forcing $R \neq 0$ so a and b are not zero-divisors. Therefore $R - \{0\}$ is closed under multiplication and so it is a semigroup with left identity and left inverses so it has a multiplicative group structure. Therefore R is a division ring. $\square$

Now to the exercise. **Proof:** Suppose J is not a maximal left ideal – that is the same as suppose there are more than one such ideals. Then J is properly contained in any maximal left ideal, say for instance M. As such R/J has a proper left ideal M/J by the correspondence theorem; hence, R/J is not a division ring. So by the contrapositive, if R/J is a division ring then R has exactly one maximal left ideal.

If R has a unique maximal left ideal then it is precisely the Jacobson radial. Also as J is maximal it follows R/J has no proper left ideals. Since R/J has an identity and no proper left ideals it follows it is a division ring. We prove this with as a lemma. $\square$

Hint: Consider $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

76 Division Rings – True or False? If R is a semi-simple artinian ring with $r^3 = r$ for all $r \in R$, then R is a division ring.

Example: False. Notice if $r^3 = r$ for all r then $0 = r(r^2 - 1)$ for all r. If $r \neq 0$ and $r^2 \neq 1$, then r is a zero-divisor in which case R would not be a division ring. This means everything must have order 2.

Now we simply look for a semi-simple ring without this property. For instance, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is semi-simple artinian as it is a product of fields. Moreover

$(a,b)^3 = (a^3,b^3) = (a,b)$. Yet clearly $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ under componentwise multiplication is not a field or a division ring as it has zero-divisors: $(1,0)\cdot(0,1) = (0,0)$. □

77 Complex dimension 4 Algebras – True or False? If A and B are semi-simple artinian complex algebras of dimension 4 then $A \cong B$.

Hint: Use the Wedderburn-Artin theorem to describe the possibilities.

Example: False. By the Wedderburn-Artin theorem we know $R = \mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}$ and $S = M_2(\mathbb{C})$ are complex semi-simple artinian algebras. However R has non-trivial two sided ideals while S is a simple ring. Therefore R is not congruent to S. □

78 Complex dimension 3 Algebras – True or False? If A and B are semi-simple artinian complex algebras of dimension 3 then $A \cong B$.

Hint: Use the Wedderburn-Artin theorem to describe the possibilities.

Proof: True. By the Wedderburn-Artin theorem we know that any complex dimension 3 algebra must decompose as follows:

$$A \cong M_{n_1}(D_1)\oplus\cdots\oplus M_{n_k}(D_k), \qquad n_1^2 dim_{\mathbb{C}} D_1 + \cdots + n_k^2 dim_{\mathbb{C}} D_k = dim_{\mathbb{C}} A = 3.$$

As no perfect square is less than 3, save 1, it follows each $n_i = 1$. Now recall from Exercise-3.74 that any finite dimensional simple algebra over $\mathbb{C}$ has a perfect square for its dimension. Since neither 2 nor 3 are perfect squares there are no division rings over dimension 2 or 3 over $\mathbb{C}$. It follows the rings take the form

$$\mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}$$

and so they are all isomorphic. □

79 Rings of idempotents If R is a left semi-simple artinian ring with $r^2 = r$ for all $r \in R$ then R is isomorphic to a direct product of of copies of $\mathbb{F}_2$.

Hint: Notice that all non-zero non-unital idempotents are zero-divisors.

Proof: Since R is semi-simple artinian by the Wedderburn-Artin it takes the form

$$R \cong M_{n_1}(D_1)\oplus\cdots\oplus M_{n_k}(D_k).$$

If any $n_i > 1$ then there exists non-trivial nilpotent matrices which clearly are not idempotent. So we restrict ourselves to having $n_i = 1$ for each i.

Next suppose $1 < |D_i| = n \neq 2$. Then pick and $r \in D_i$ which is not 0 or 1. Clearly the fact that $r^2 = r$ implies $0 = r(1-r)$ proving r is a zero-divisor. Hence $|D_i| = 2$. As such it is precisely the field $\mathbb{F}_2$. In conclusion, R is a finite direct sum of $\mathbb{F}_2$'s. □

80 Nilpotent Free Rings – True or False? If R is an artinian ring having no non-zero nilpotent elements then R is a direct sum of fields.

Hint: Consider any non-commutative division ring.

Example: False. Take any division ring, for instance the Hamiltonians . As $^\times$ there can be no non-zero zero-divisors, let alone nilpotent elements. As every division ring has no proper left ideals it is trivially artinian as well. Furthermore, division rings are simple rings so they cannot be isomorphic to any non-trivial ring product. As itself is not a field we see indeed the claim is false. □

81 Real Algebras of Dimension 2 Classify all 2-dimensional $\mathbb{R}$-algebras.

Hint: When the Jacobson radical is not trivial the algebra is $\mathbb{R}[x]/(x^2)$. Do not forget to show there are no division rings of dimension 2 over $\mathbb{R}$ which are not $\mathbb{C}$.

Proof: Let A be a 2-dimensional $\mathbb{R}$-algebra.

As $\mathbb{R}$ is a field it follows any finite dimensional $\mathbb{R}$ algebra is artinian. If the Jacobson radical is non-trivial then to be proper it must have dimension 1 over $\mathbb{R}$. As A is also artinian it follows $J(A)$ is nilpotent and so indeed $J(A)^2 = \mathbf{0}$.

Select a basis that extends 1, so $\{1, \alpha\}$. It follows every element takes the form $a_1 + a_2\alpha$. So consider $\alpha^2 = a_0 + a_1\alpha$.

If $a_0 = 0$ and $a_1 = 0$. Then $\alpha^2 = 0$ in which case there is a natural surjection from $\mathbb{R}[x]/(x^2)$ onto A by sending $x \mapsto \alpha$. With little effort this is seen as injective as well. This is the case when there is not a trivial Jacobson radical.

Now consider $a_1 \neq 0$. Suppose $b_0 + b_1\alpha$ is a nilpotent element of order 2.

$$\begin{aligned} 0 &= (b_0 + b_1\alpha)^2 \\ &= b_0^2 + 2b_0b_1 + b_1^2\alpha^2 \\ &= (b_0^2 + b_1^2a_0) + (2b_0b_1 + b_1^2a_1)\alpha. \end{aligned}$$

Since $\{1, \alpha\}$ is a basis it follows

$$b_0^2 + b_1^2a_0 = 0, \qquad 2b_0b_1 + b_1^2a_1 = 0.$$

In the first we see $b_0^2 = -b_1^2a_0$, and so a_0 must be a square as well. However in $\mathbb{R}$ all squares are non-negative so $0 \leq b_0^2 = -(b_1\sqrt{a_0})^2$. The problem is that $(b_1\sqrt{a_0})^2 \geq 0$ as well. Therefore $0 = b_0$ and either $b_1 = 0$ or $a_0 = 0$. If it is the former we are done, if it is the latter we return to $2b_0b_1 + b_1^2a_1 = 0$ and notice we need only ask when $b_1^2a_1 = 0$. Since we assumed $a_1 \neq 0$ we see indeed $b_1 = 0$. Therefore all nilpotent elements of order 2 are trivial. Hence $J(A) = \mathbf{0}$.

In the other case that $J(A) = \mathbf{0}$, it follows A is semi-simple artinian. Hence

$$A \cong \mathbb{R} \oplus \mathbb{R}, \qquad A \cong \mathbb{C}, \qquad A \cong D$$

where D is some division ring of dimension 2 over $\mathbb{R}$. It remains to show that any dimension 2 division ring over $\mathbb{R}$ is isomorphic to $\mathbb{C}$.

Given $\{1, \alpha\}$ as a basis of D over $\mathbb{R}$ consider the product $r\alpha$ for any $r \in \mathbb{R}$. Since $\mathbb{R}$ is in the center of D it follows $r\alpha = \alpha r$. Now take any two elements $(a + b\alpha), (c + d\alpha) \in D$.

$$(a+b\alpha)(c+d\alpha) = ac+ad\alpha+b\alpha c+b\alpha d\alpha = ca+bc\alpha+d\alpha a+d\alpha b\alpha = (c+d\alpha)(a+b\alpha).$$

Thus any 2-dimensional division algebra over $\mathbb{R}$ is a field. As such it is $\mathbb{C}$.

So the list of 2-dimensional $\mathbb{R}$-algebras up to isomorphism is:

$$\mathbb{R}[x]/(x^2), \qquad \mathbb{R} \oplus \mathbb{R}, \qquad \mathbb{C}.$$

□

Hint: Determine the companion matrices.

82 Similar Matrices Determine whether or not the matrices

$$A = \begin{bmatrix} 1 & 3 & 1 \\ 2 & 2 & -1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 0 & -6 \\ 1 & 0 & 1 \\ 0 & 1 & 4 \end{bmatrix}$$

are similar over rationals.

Example: Since $\mathbb{Q}$ is not algebraically closed it is possible that some of the eigenvalues are not in $\mathbb{Q}$ and as such we may not use the Jordan Canonical form. Instead we use invariant factors and the rational canonical form.

First we find the characteristic polynomial to be

$$\chi_A(\lambda) = \lambda^3 - 4\lambda^2 - \lambda + 6, \qquad \chi_B(\lambda) = \lambda^3 - 4\lambda^2 - \lambda + 6.$$

Notice in fact B is the companion matrix of χ_A and χ_B.

By the rational root test there are no rational roots so we know χ_A is irreducible and so the minimal polynomial must equal χ_A. Hence A is similar only to matrices whose companion matrix is precisely the same as $C(\chi_A)$. As noted above, B is such a matrix. So A and B are similar. $\square$

83 Similar Matrices Determine whether or not the matrices

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 2 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & -5 \end{bmatrix}$$

are similar over rationals.

Hint: Determine the companion matrices.

Example: Since $\mathbb{Q}$ is not algebraically closed it is possible that some of the eigenvalues are not in $\mathbb{Q}$ and as such we may not use the Jordan Canonical form. Instead we use invariant factors and the rational canonical form.

Notice that A^T is a companion matrix for $p(x) = x^3 - x^2 - 2x + 1$. As A is similar to A^T it follows are have the invariant factors of A. For B we simply compute it directly as:

$$\chi_B(x) = (x+5)(x^2 - 3x - 2).$$

By the rational roots test we find $p(x)$ to be irreducible over $\mathbb{Q}$ so it is the lone invariant factor. As $\chi_B(x)$ is reducible, so is the minimal polynomial and so indeed A and B do not have the same invariant factors. Hence they are not similar. (Indeed the minimal polynomial for B is χ_B.) $\square$

84 Nilpotent Matrices An $n \times n$ nilpotent matrix with entries in a field has characteristic polynomial x^n.

Hint: Find the minimal polynomial of nilpotent matrix.

Proof: Take a nilpotent $n \times n$ matrix A. Assume that $A^k = 0$ for some the least k. It follows x^k is the minimal polynomial for A. As such x^k divides the characteristic polynomial. But we also know that all the roots of the characteristic polynomial are roots of the minimal polynomial, so there can only be 0 eigenvalues. Hence, x^n is the characteristic polynomial. $\square$

85 Similarity Classes – True or False? There are exactly 3 similarity classes of 4×4 matrices A over $\mathbb{F}_2$ satisfying $A^2 = 1$.

Hint: Consider invariant factors.

Example: True. We see that the minimal polynomial of A must divide $x^2 - 1$. Over $\mathbb{F}_2$ this allows for the following factors two factors:

$$x - 1, \qquad x^2 - 1.$$

Therefore we have the following choices of invariant factors:

$$x-1|x-1|x-1|x-1, \qquad x-1|x-1|x^2-1, \qquad x^2-1|x^2-1.$$

As invariant factors uniquely describe each similarity class we see we have only 3 similarity classes with the property that the matrices by 4×4 and the minimal polynomial divide $x^2 - 1$. $\square$

86 Similarity Class of $\mathbb{F}_2$ Give a list of 2×2 matrices over $\mathbb{F}_2$ such that every 2×2 matrix over $\mathbb{F}_2$ is similar to exactly one on your list.

Hint: Consider all possible minimal polynomials and then from these all possible invariant factors.

Example: Over $\mathbb{F}_2$ the number of polynomials of degree 2 or less is few and each is allowed as a minimal polynomial of 2×2 matrices over $\mathbb{F}_2$ – in fact they uniquely exhaust the possibilities. Therefore we fix a minimal polynomial and find the associated invariant factors the end with this minimal polynomial and then move on.

The coefficients of the polynomials of degree less than or equal to 2 correspond to all length 3 binary words – excluding 000 and 001:

$$a(x) = x, \qquad b(x) = x+1, \qquad c(x) = x^2,$$

$$d(x) = x^2+1, \qquad e(x) = x^2+x, \qquad f(x) = x^2+x+1.$$

Now their associated invariant factors with the added condition that the total degree fo the product of the invariant factors equal 2 so that the companion matrices fit in 2×2 matrices.

$$\begin{aligned} x|x &\rightarrow \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}; \\ x+1|x+1 &\rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \\ x^2 &\rightarrow \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}; \\ x^2+1 &\rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \\ x^2+x &\rightarrow \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}; \\ x^2+x+1 &\rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}. \end{aligned}$$

□

Hint: Consider the eigenspaces of φ and ψ.

87 Simultaneous Diagonalization Let V be a finite dimensional vector space and let φ and ψ be commuting diagonalizable linear transformations from V to V. Show that φ and ψ can be simultaneously diagonalized.

Proof: If a finite dimensional linear transformation is diagonalizable over its field then it has all its eigenvalues in the field (under some basis the matrix is diagonal and the eigenvalues are simply those elements on the diagonal.)

If all the eigenvalues of a linear transform are the same then the associated diagonal matrix is scalar. If both φ and ψ are scalar then they are both simultaneously diagonalized.

Now presume that without loss of generality that φ is not a scalar transform. Hence there are at least two distinct eigenspaces. It follows each eigenspace of φ has dimension less than that of V. Since $\varphi(E_i) = E_i$ for any eigenspace E_i we see that in fact that since φ and ψ commute they leave each others eigenspaces invariant – consider restricting to some eigenspace E_i of φ.

Now we setup an induction. When the dimension of V is 1, all linearly transformations are scalar (Schur's lemma). Suppose that for all vector spaces of dimension n, any commuting diagonalizable linear transformations can be simultaneously diagonalized. Then in the case where $dim\ V = n+1$, either all the two linear transformations are scalar and so simultaneously diagonalized, or one is not scalar in which case its eigenspaces are proper subspaces. So we restrict the maps to any eigenspace and by induction simultaneously diagonalize on the this subspace. That the maps commutate means that they respect each others eigenspaces and as such we can do this for all eigenspaces of V under the non-scalar map until in the end we have both maps simultaneously diagonalized.

□

88 Simultaneous Diagonalization Let V be a finite dimensional vector space and let $\{\varphi\}_{i\in I}$ be a family of commuting diagonalizable linear transformations from V to V. Show that φ_i can be simultaneously diagonalized.

Hint: Consider the eigenspaces of φ_i.

Proof: If a finite dimensional linear transformation is diagonalizable over its field then it has all its eigenvalues in the field (under some basis the matrix is diagonal and the eigenvalues are simply those elements on the diagonal.)

If all the eigenvalues of a linear transform are the same then the associated diagonal matrix is scalar. If all φ_i are scalar then they are both simultaneously diagonalized.

Now presume that without loss of generality that φ_i is not a scalar transform. Hence there are at least two distinct eigenspaces. It follows each eigenspace of φ_i has dimension less than that of V. Since $\varphi_i(E_j) = E_j$ for any eigenspace E_j we see that in fact that since all φ_i commute they leave each others eigenspaces invariant – consider restricting to some eigenspace E_i of φ_i.

Now we setup an induction. When the dimension of V is 1, all linearly transformations are scalar (Schur's lemma). Suppose that for all vector spaces of dimension n, any commuting diagonalizable linear transformations can be simultaneously diagonalized. Then in the case where $dim\ V = n + 1$, either all the two linear transformations are scalar and so simultaneously diagonalized, or one is not scalar in which case its eigenspaces are proper subspaces. So we restrict the maps to any eigenspace and by induction simultaneously diagonalize on the this subspace. That the maps commutate means that they respect each others eigenspaces and as such we can do this for all eigenspaces of V under the non-scalar map until in the end we have both maps simultaneously diagonalized.
□

89 Matrices and Polynomials Let V be a 7-dimensional vector space over $\mathbb{Q}$.

Hint: Construct the companion matrices of the invariant factors to match dimension 7.

(a) How many similarity classes of linear transformations on V have characteristic polynomial $(x-1)^4(x-2)^3$?

(b) Of the similarity classes in (a), how many have minimal polynomial $(x-1)^2(x-2)^3$?

(c) Let φ be a linear transformation from V to V having characteristic polynomial $(x-1)^4(x-2)^3$ and minimal polynomial $(x-1)^2(x-2)^3$. Find $dim\ ker\ (\varphi - 2id)$.

Example:

(a) Let $a = (x-1)$ and $b = (x-2)$. Having fixed the characteristic polynomial we look at the possible invariant factors that give this polynomial. We now the final invariant factor is the minimal polynomial so it must have all the roots of the characteristic. Thus both a and b divide the final term.

Let $a_1, \dots, a_k$ denote the powers of a in the order of the invariant factors, and likewise $b_1, \dots, b_l$ the powers for b. The algorithm to traverse each invariant factor chain is given by the relations,

$$1 \leq a_1 \leq \cdots \leq a_k \leq 4, \qquad 1 \leq b_1 \leq \cdots \leq b_l \leq 3,$$

$$a_1 + \cdots + a_k = 4, \quad \text{and} \quad b_1 + \cdots + b_l = 3.$$

Notice the last two always force

$$a_1 + \cdots + a_k + b_1 + \cdots + b_l = 7$$

so that we need not explicitly make use of the fact that we have 7-dimensional space.

This gives the following possible chains for a_i's:

$$A = \begin{array}{||c||c||c||c||} \hline 1,1,1,1 & 1,1,2 & 1,3 & 1,4 \\ \hline & 2,2 & & \\ \hline \end{array}$$

For b_j's we get

$$B = \begin{array}{||c||c||c||} \hline 1,1,1 & 1,2 & 3 \\ \hline \end{array}$$

Thus the total number of configurations is the product of the configurations possible for a and b. This gives a total of 15. For clarity they are enumerated below

$$\begin{array}{rccccccc}
A_{1,1} + B_1: & a & \mid & ab & \mid & ab & \mid & ab \\
A_{1,1} + B_2: & a & \mid & a & \mid & ab & \mid & ab^2 \\
A_{1,1} + B_3: & a & \mid & a & \mid & a & \mid & ab^3 \\
A_{1,2} + B_1: & & & ab & \mid & ab & \mid & a^2b \\
A_{1,2} + B_2: & & & a & \mid & ab & \mid & a^2b^2 \\
A_{1,2} + B_3: & & & a & \mid & a & \mid & a^2b^3 \\
A_{2,2} + B_1: & & & b & \mid & a^2b & \mid & a^2b \\
A_{2,2} + B_2: & & & & & a^2b & \mid & a^2b^2 \\
A_{2,2} + B_3: & & & & & a^2 & \mid & a^2b^3 \\
A_{1,3} + B_1: & & & b & \mid & ab & \mid & a^3b \\
A_{1,3} + B_2: & & & & & ab & \mid & a^3b^2 \\
A_{1,3} + B_3: & & & & & a & \mid & a^3b^3 \\
A_{1,4} + B_1: & & & b & \mid & b & \mid & a^4b \\
A_{1,4} + B_2: & & & & & b & \mid & a^4b^2 \\
A_{1,4} + B_3: & & & & & & & a^4b^3
\end{array}$$

(b) Now assume instead that the invariant factor all conclude with a^2b^3. Ignoring the possible characteristic polynomials what are our options. We redesign our algorithm slightly. The information that is missing now is what the total multiplicity of powers is. We do however now the dimension of our space to be 7 so we can add this to our defining relations as follows:

$$1 \le a_1 \le \cdots \le a_k = 2, \qquad 1 \le b_1 \le \cdots \le b_l = 3,$$

$$a_1 + \cdots + a_k + b_1 + \cdots + b_l = 7.$$

If, for instance, we look at the a_i's separately we notice the length k is not restricted. Thus we must make sure of the final relation each time. Indeed we see the subrelation

$$a_1 + \cdots + a_{k-1} + b_1 + \cdots + b_{l-1} = 2.$$

This means $1 \le k - 1 + l - 1 \le 2$ or simply $3 \le k + l \le 4$. Our options are $k = 1$, $l = 2, 3$; $l = 1$, $k = 2, 3$; or $k = l = 2$. Thus we get the possibilities

$$b^2|a^2b^3, \qquad b|b|a^2b^3, \qquad a^2|a^2b^3, \qquad a|a|a^2b^3, \qquad ab|a^2b^3.$$

There are 5 similarity classes with minimal polynomial a^2b^3.

(c) Now we combine our results and notice that when a^4b^3 is the characteristic polynomial and a^2b^3 the minimal polynomial, then the only choices for invariant factors are

$$a|a|a^2b^3, \qquad a^2|a^2b^3.$$

To calculate the dimension of the null-space of the eigenspace associated with the eigenvalue 2, we simply see the multiplicity of 2 is 3, so its eigen space has dimension 3, and so the nullity is of dimension 3.

□

90 Minimal Polynomials Exhibit a 4×4 matrix A with integer coefficients such that $A^5 = I_4 \neq A$.

Hint: Notice the minimal polynomial for any such A divides $x^5 - 1$.

Example: As the relation $A^5 = I_4$ demonstrates, the minimal polynomial for A divides $x^5 - 1$. As $A \neq I_4$ it follows the factor $x - 1$ is not the contributing factor. So consider

$$p(x) = (x^5 - 1) \div (x - 1) = x^4 + x^3 + x^2 + x + 1.$$

Certainly $p(A) = 0$ still as expressed above, and also as we want a 4×4 matrix we may as well simply choose the companion matrix of $p(x)$. So take

$$A = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

As designed $A^5 = I_4$ and $A \neq I_4$. □

91 Matrix Relations Let $A, B \in M_5(\mathbb{Q})$ be non-zero 5×5 matrices over $\mathbb{Q}$ such that $AB = BA = 0$. Prove that if $A^4 = A$ and $B^4 = B^2 - B$ then $A + B$ is invertible.

Hint: Compute the possible invariant factors of A and B.

Proof: From the relation $A^4 = A$ we know the minimal polynomial of A divides $x^4 - x$, and as $A \neq 0$, it cannot be the factor x alone. Nor can it be the factor $x - 1$ as A is a zero-divisor and as such not the identity. The rational roots theorem tells us $x^2 + x + 1$ is irreducible so there are no smaller factors. However if the minimal polynomial is $x^2 + x + 1$ then the invariant factors must have a total degree which is even. As we have 5×5 matrix this cannot exist. Also if no eigen value is 0, then the product of eigenvalues is a unit in $\mathbb{Q}$ so A is invertible. However, invertible matrices are not zero-divisors. Hence we can conclude that the only possibilities for minimal polynomials are:

$$x(x - 1), \qquad x(x^2 + x + 1), \qquad x(x - 1)(x^2 + x + 1).$$

Moving to B we notice the minimal polynomial divides $x^4 - x^2 + x$, and again as $B \neq 0$ it is not only the factor x that accounts for the annihilation. So the minimal polynomial must divide contain factors from $x^3 - x + 1$. By the rational roots theorem we see $x^3 - x + 1$ is irreducible over $\mathbb{Q}$; hence, the minimal polynomial of B is precisely $x^4 - x^2 + x$. This means the stray eigen value is 0 as the other roots are outside of $\mathbb{Q}$. So the invariant factors of B are $x|x^4 - x^2 + x$.

Now we invoke the property that $AB = BA = 0$. As the transformations commute they respect each others eigenspaces.**PENDING:** finish □

92 Linear Decomposition Let V be a finite dimensional vector space over

Hint: Consider a decomposition into eigenspace first, and then a decomposition into invariant factors.

a field F. Let θ be a linear transformation on V. Assume that there do not exist proper θ-invariant subspaces V_1, V_2 of V such that $V = V_1 \oplus V_2$. Show that for some basis of V the matrix of θ is the companion matrix of $p(x)^e$, where $p(x)$ is some irreducible polynomial in $F[x]$.

Proof: The minimal polynomial of θ is a product of irreducibles in $F[x]$. If there are two are more irreducibles in the minimal polynomial, then the roots of each determine distinct eigenspaces. As eigenspaces are respected by the map from which they are determined, it follows this non-trivial decomposition is of the type forbidden by the hypothesis. So we are forced to accept that there is indeed only one irreducible component in the minimal polynomial.

Finally if there are more than one invariant factors, then we know

$$V = I_1 \oplus \cdots \oplus I_n$$

where each I_i is generated by the invariant factor i. This decomposition is also clearly respected by θ as it describes θ. Therefore there can only be on invariant factor and this invariant factor must be the minimal polynomial which we recently decided was simply a power of an irreducible in $F[x]$. □

Hint:

93 Jordan Normal Form Let V be a finite dimensional vector space over $\mathbb{Q}$. Let θ be a linear transformation on V having characteristic polynomial $(x-2)^4$.

(a) Describe the possible Jordan normal forms for θ, and for each of these give the minimal polynomial of θ.

(b) For each of the possibilities in (a) give the dimension of the 2-eigenspace of θ.

(c) Assume that θ leaves invariant only finitely many subspaces of V. What can be said about the Jordan normal form of θ?

Example: PENDING: find the energy to do this one. □

Hint: Use the fact that $J(R)$ annihilates all simple R-modules.

94 Jacobson Module Let R be an artinian ring. Show that $J(R)$ is a semi-simple left R-module if and only if $J(R)^2 = \mathbf{0}$.

Proof: Let $V = J(R)$ be a semi-simple left R-module. Suppose that

$$V = V_1 \oplus \cdots \oplus V_n$$

is the decomposition into simple R-modules. From Nakayama's Lemma we know if $J(R)V_i = V_i$ then $V_i = \mathbf{0}$. Since each V_i is simple as an R-module, it follows $J(R)V_i = \mathbf{0}$ for each i. This means that $J(R)V = 0$. But now recall that $V = J(R)$ and we see that indeed $J(R)^2 = \mathbf{0}$.

Now suppose that $J(R)^2 = \mathbf{0}$. It is clear that $J(R)$ is contained in the annihilator of $V = J(R)$, and as $J(R)^2 = \mathbf{0}$ it is in fact the annihilator. Therefore $J(R)$ is a faithful $R/J(R)$-module. However, R is artinian, so $R/J(R)$ is semi-simple artinian. Thus every left $R/J(R)$-module is semi-simple. Now we observe that we can use this decomposition into simple $R/J(R)$-modules back to R-modules since $J(R)$ annihilates all simple R-modules. Hence, V is a semi-simple R-module, that is, $J(R)$ is a semi-simple R-module. □

Hint: Note R is a matrix ring over a division ring.

95 Simple Algebras Suppose that R is a finite dimensional simple F-algebra, for a field F. Show that $dim_F\ R = n^2 e$, where $ne = dim_F\ V$ for some irreducible R-module V.

Proof: Since are R is a finite dimensional simple F-algebra it follows it is semi-simple artinian so indeed

$$R \cong M_n(D).$$

Furthermore, D is an F-algebra and finite dimensional as well. However, as soon as we fill one component in a matrix, then to generate the full left ideal we need to include the entire column. Thus we get a natural copy of $V = D^n$ as an irreducible R-module – irreducible because it is a minimal left ideal of R. Finally letting $e = dim_F\ D$ we see:

$$dim_F\ R = n^2 e, \qquad dim_F\ V = ne.$$

□

96 Endomorphisms and Semi-simplicity Let F be a field and V be a finite dimensional F-vector space. Let $\theta \in End_F(V)$ have minimal polynomial $f(x) \in F[x]$. Let R be the subalgebra $F[\theta]$ of $End_F(V)$. Prove that R is semi-simple artinian if and only if each prime factor of $f(x)$ in $F[x]$ has multiplicity 1.

Hint:

Proof: Suppose R is semi-simple artinian.

By the theorem of Wedderburn-Artin we decompose R as

$$R = F[\theta] = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k).$$

Since V is an $F[x]$-modules it also passes as an R-module. Moreover, it then follows that V is an $M_{n_i}(D_i)$-module.

In a PID primes correspond to irreducibles so we simply wish to prove that $f(x)$ is a product $p_1(x) \cdots p_n(x)$ with each $p_i(x)$ irreducible and $p_i(x) = p_j(x)$ implying $i = j$.

PENDING: figure it out. □

97 Indecomposable Modules – True or False? For a short exact sequence

Hint: Consider a cyclic group with zero-divisors.

$$\mathbf{0} \longrightarrow V \longrightarrow W \longrightarrow X \longrightarrow \mathbf{0}$$

if V and W are indecomposable then so is X.

Example: False. Consider the following sequence of $\mathbb{Z}$-modules:

$$\mathbf{0} \longrightarrow \mathbb{Z} \xrightarrow{6} \mathbb{Z} \longrightarrow \mathbb{Z}_6 \longrightarrow \mathbf{0}\ .$$

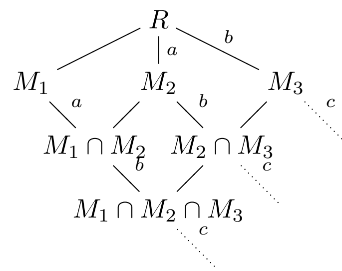
As $\mathbb{Z}$ has no zero-divisors it can have no idempotents and so it is indecomposable. Yet clearly as $\mathbb{Z}$-modules $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. □

98 Maximal Ideals Show that if $M_1, M_2, \ldots, M_n$ are distinct maximal ideals of the commutative ring R, then each R-module R/M_i, $1 \leq i \leq n$, is isomorphic to exactly one factor of the chain

Hint: Use the third isomorphism theorem.

$$R \geq M_1 \geq M_1 \cap M_2 \geq \cdots \geq M_1 \cap M_2 \cap \cdots \cap M_n.$$

Proof: With the correct picture the result is an obvious interpretation of the third isomorphism theorem.



We simply recurse.

$$R/M_i \cong M_{i-1}/M_{i-1} \cap M_i \cong M_{i-2} \cap M_{i-1}/M_{i-2} \cap M_{i-1} \cap M_i \cong \cdots$$
$$\cong M_1 \cap \cdots M_{i-1}/M_1 \cap \cdots \cap M_i.$$

As each M_i is distinct, so is each R/M_i and so each factor of the chain is uniquely one of the R/M_i's. □

Hint:

99 Polynomial Rings – True or False? If R is a commutative artinian ring then $R[x]$ is noetherian.

Proof: True.[9]
□

Hint: Show it is divisible.

100 Injective Modules – True or False? $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

Proof: Since $\mathbb{Z}$ is a PID it is sufficient to show $\mathbb{Q}$ is divisible. This means for every $n \in \mathbb{Z}$, $n\mathbb{Q} = \mathbb{Q}$. Certainly for every fraction $a/b \in \mathbb{Q}$ the fraction a/nb is also in $\mathbb{Q}$ and thus $n(a/nb) = a/b$ proving $n\mathbb{Q} = \mathbb{Q}$. So $\mathbb{Q}$ is an injective $\mathbb{Z}$-modules as it is divisible. □

Hint: For (ii) implies (iii) use $P = W$, for (iii) implies (iv) use the retract of the split sequence, for (iv) implies (ii) use the pull-back of the diagram.

101 Non-projective Modules Give three different definitions of projective modules and show that your definitions are equivalent.

Theorem 3.0.11 *All the following are equivalent in the category of left R-modules:*

(i) P is a projective R-module.

(ii) Given any map $\varphi : P \to W$ and another surjective map $f : V \to W$, then there exists a map $\psi : P \to V$ such that the following diagram commutes:

$$\begin{tikzcd} & P \arrow[dl, dashed, "\psi"'] \arrow[d, "\phi"] & \\ V \arrow[r, "f"'] & W \arrow[r] & \mathbf{0}. \end{tikzcd}$$

(iii) Every short exact sequence:

$$\mathbf{0} \longrightarrow U \longrightarrow V \xrightarrow{f} P \longrightarrow \mathbf{0}$$

splits.

[9]By the Hilbert basis theorem, $R[x]$ is noetherian because R is commutative and noetherian.

(iv) *If P is a quotient module of V then it is also a direct summand of V; so there exists an embedding $P' \cong P$ in V and a complement U such that $V = P' \oplus U$.*

Proof: (i) implies (ii) and (ii) implies (i) by the very definition of projective modules.

Now consider why (ii) implies (iii). If we take a short exact sequence

$$\mathbf{0} \longrightarrow U \longrightarrow V \xrightarrow{f} P \longrightarrow \mathbf{0}$$

and let W in (ii) be equal to P, together with $\varphi = id_P$, then we immediately have the picture:

$$\begin{tikzcd} & & & P \arrow[dl, "\psi"'] \arrow[d, leftrightarrow, "id_P"] & \\ \mathbf{0} \arrow[r] & U \arrow[r] & V \arrow[r, "f"] & P \arrow[r] & \mathbf{0}. \end{tikzcd}$$

As (ii) tells us, $\psi f = id_P$. However this is an equivalent condition for a short exact sequence to be split exact – we now have a retract ψ. Therefore (ii) implies (iii).

Assume (iii) now and let P be a quotient of a module V. It follows we we have surjection $f : V \to P$ with kernel U. Thus we have the short exact sequence:

$$\mathbf{0} \longrightarrow U \longrightarrow V \xrightarrow{f} P \longrightarrow \mathbf{0}.$$

From our assumption of (iii) we know this short exact sequence splits so indeed P can be embedded in V as a direct summand – (iv).

Finally assume (iv) is true, and assume we have a surjection $f : V \to W$ and a map $\varphi : P \to W$. Then consider the pull-back of the diagram:

$$\begin{tikzcd} & P \arrow[d, "\phi"] & \\ V \arrow[r, "f"'] & W \arrow[r] & \mathbf{0}, \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "\pi_P"] \arrow[d, "\pi_V"'] & P \arrow[d, "\phi"] & \\ V \arrow[r, "f"'] & W \arrow[r] & \mathbf{0} \end{tikzcd}$$

where $X = \{(v,p) \in V \oplus P \; : \; f(v) = \phi(p)\}$ and where $\pi_P(v,p) = p$ and $\pi_V(v,p) = v$. Given any $p \in P$, $\phi(p) \in W$ so there exists a $v \in V$ such that $f(v) = \phi(p)$. Hence $(v,p) \in X$ and $\pi_P(v,p) = p$ proving that π_P is surjective. Therefore P splits in X by the assumption of (iv). Use the map $i : P \to X$ as the retract for π_P. Then we see the composition $\pi_V i : P \to V$ and furthermore,

$$f\pi_V i(p) = f(\pi_V(v,p)) = f(v) = \phi(p)$$

by design. So the diagram commutes:

$$\begin{tikzcd} & P \arrow[dl, "\pi_V i"'] \arrow[d, "\phi"] & \\ V \arrow[r, "f"'] & W \arrow[r] & \mathbf{0}. \end{tikzcd}$$

Therefore P is projective. $\square$

102 Projective $\mathbb{Z}$-modules Prove $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module by

Hint: Suppose $\mathbb{Z} < \mathbb{Q} < F$ the consider $F/\mathbb{Z} > \mathbb{Q}/\mathbb{Z}$ and the torsion of each quotient module.

showing it is not a direct summand of a free $\mathbb{Z}$-module.

Proof: [10] Suppose F is any free $\mathbb{Z}$-module containing $\mathbb{Q}$. As it stands, $F \cong \oplus_i \mathbb{Z}$. Since $\mathbb{Q}$ is embedded in F, we may take the principle copy of $\mathbb{Z}$ inside $\mathbb{Q}$ and create a tower of $\mathbb{Z} \leq \mathbb{Q} \leq F$ through which we quotient by $\mathbb{Z}$ to obtain: $F/\mathbb{Z} \geq \mathbb{Q}/\mathbb{Z}$.

$\mathbb{Q}/\mathbb{Z}$ corresponds to the rational points on the unit circle so we visibly have an infinite amount of torsion; more specifically, we have torsion of every positive order. However, given any $\mathbb{Z}$ embedded in F, there corresponds a generator $v \in F$, such that $\mathbb{Z} = \mathbb{Z}v$ in F. Yet F is a direct sum, so v must be almost everywhere 0. This means no matter how large F is, we can only factor out, non-trivially, a finite number of components. So while factors exist that create torsion, there is insufficient to create the infinite amount that is created by quotienting $\mathbb{Q}$ by $\mathbb{Z}$. Thus $\mathbb{Q}/\mathbb{Z}$ cannot be a submodule of $F/\mathbb{Z}$ so by the correspondence theorem, $\mathbb{Q}$ is not embedded in F and hence cannot be a direct summand either. $\square$

Hint: Show that they contain $\mathbb{Q}$ and that $\mathbb{Q}$ is not contained in a free module (Exercise-3.102.)

103 Non-projective Modules Show a field of characteristic 0 is not a projective $\mathbb{Z}$-module under the regular action.

Proof: Every field of characteristic 0 contains a subfield isomorphic to $\mathbb{Q}$. However, from Exercise-3.102, $\mathbb{Q}$ is not a direct summand of a free $\mathbb{Z}$-module. Moreover, the proof indicates that $\mathbb{Q}$ is indeed not even a submodule of a free $\mathbb{Z}$-module. Hence, no field of characteristic 0 is a submodule of a free $\mathbb{Z}$-module and hence it may not be a direct summand of a free $\mathbb{Z}$-module. This characterization describes all projective modules; thus, no field of characteristic 0 is a projective $\mathbb{Z}$-module. $\square$

Hint: Only $\mathbf{0}$ and R work.

104 Cyclic Projective Modules Let R be a PID. Which cyclic R-modules are projective?

Example: Let $V = Rv$ be a cyclic R-module. Without loss of generality assume $V \neq \mathbf{0}$.

Define the map $f : R \to Rv$ by $f(x) = xv$. Since

$$f(rx + y) = (rx + y)v = r(xv) + yv = rf(x) + f(y)$$

and multiplication is well-defined, we have a nice R-linear map. Also, any $xv \in Rv$ is clearly hit by x, so f is surjective. Finally if the kernel of f is trivial then we attain an isomorphism of R-modules. Thus $R \cong Rv$ whenever $xv = 0$ implies $x = 0$.

So we may say, any cyclic R-module with trivial annihilator is projective, simply because it is isomorphic to R as a regular left R-module, and R is free as an R-module.

Now assume $Ann(V) \neq 0$, so the kernel is non-trivial; then $rv = 0$ for some non-zero $r \in R$. Thus V contains torsion elements by definition. However, free R-modules must be torsion free, so they cannot contain V as a submodule, let alone as a direct summand. Hence such cyclic modules are not projective. $\square$

Hint: The category of $\mathbb{Z}_4$-modules provides all the necessary counter-examples.

105 Projective/Injective Inheritance Let R be commutative. Prove or Disprove:

(i) Every submodule of a projective R-module is projective.

[10] An equivalent way to show $\mathbb{Q}$ is not projective is to observe every projective module over a PID is free. Yet $\mathbb{Q}$ is not free as any two rational numbers are linearly dependent over $\mathbb{Z}$.

(ii) Every submodule of and injective R-module is injective.

(iii) Every quotient of a projective R-module is projective.

(iv) Every quotient of a injective R-module is injective.

Example: Let $R = \mathbb{Z}/4$. Consider the short exact sequence:

$$\mathbf{0} \longrightarrow \mathbb{Z}/2 \longrightarrow \mathbb{Z}/4 \longrightarrow \mathbb{Z}/2 \longrightarrow \mathbf{0}\ .$$

It does not split as $\mathbb{Z}/4$ is not isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. However as it does not split we see the $\mathbb{Z}/2$ as $\mathbb{Z}/4$-module is not projective because it is the left term of a short exact sequence that does not split. Visibly, $\mathbb{Z}/2$ is both a submodule and a quotient modules of a projective module (the ring is always a free module under the regular action, and thus projective), but it itself is not projective.

If we can show that $\mathbb{Z}/4$ is injective over itself we will be able to conclude that $\mathbb{Z}/2$ is not an injective module as the sequence does not split, and it is the left term of the sequence. Thus, neither as a submodule, nor as a quotient is it injective. To show $\mathbb{Z}/4$ is injective requires only that we show it is injective on left ideals of $\mathbb{Z}/4$, namely, $\mathbf{0}, 2\mathbb{Z}/4$, and $\mathbb{Z}/4$. Fix the picture:

$$\begin{tikzcd} & \mathbb{Z}/4 & \\ \mathbf{0} \arrow[r] & L \arrow[u, "f"] \arrow[r, "i"] & \mathbb{Z}/4 \arrow[ul, dashed, "g"'] \end{tikzcd}$$

Since $Hom_{\mathbb{Z}/4}(\mathbf{0}, \mathbb{Z}/4) = \mathbf{0}$, when $L = \mathbf{0}$ we see $f = 0$ so we extend the map with the trivial map: $g(x) = 0$.

Now suppose the left ideal is $\mathbb{Z}/2$. Now $Hom_{\mathbb{Z}/4}(\mathbb{Z}/2, \mathbb{Z}/4)$ has only two maps: the trivial map and inclusion. If f is the trivial map then g is trivial and properly extends f. When f is inclusion, we let g be the identity map.

Finally suppose the left ideal is $\mathbb{Z}/4$ itself. Here we trivially let $f = g$. Since these extensions work for all left ideals, it proves by Baer's Criterion that $\mathbb{Z}/4$ is injective over itself. □

106 Injective $\mathbb{Z}/n\mathbb{Z}$-modules Let $n \geq 1$. Then $\mathbb{Z}/n\mathbb{Z}$ is injective $\mathbb{Z}/n\mathbb{Z}$-module.

Hint: Any cyclic module homomorphism is determined by where the generator is sent.

Proof: We make use of Baer's Criterion. The (left) ideals of $\mathbb{Z}/n\mathbb{Z}$ are $m\mathbb{Z}/n\mathbb{Z}$. Thus we need only consider extending our maps

$$\begin{tikzcd} & \mathbb{Z}/n\mathbb{Z} & \\ \mathbf{0} \arrow[r] & m\mathbb{Z}/n\mathbb{Z} \arrow[u, "f"] \arrow[r, "i"] & \mathbb{Z}/n\mathbb{Z} \arrow[ul, dashed, "g"'] \end{tikzcd}$$

Since everything is cyclic, we notice f is determined by where m is mapped, say $f(m) = k$. To be defined, m must divide n and so $n = am$ and thus $0 = f(am) = af(m) = ak$, so indeed $am|ak$ and $m|k$. Hence, $k = lm$ for some l, so f is multiplication by l. Define $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $g(x) = lx$. Certainly this is $\mathbb{Z}/n\mathbb{Z}$-linear and also agrees with f on $m\mathbb{Z}/n\mathbb{Z}$. As any left ideal map can be extended, $\mathbb{Z}/n\mathbb{Z}$ is injective. □

107 Injective $\mathbb{Z}$-modules – True or False? Every abelian group monomorphism $Z_{p^\infty} \to A$ splits.

Hint: Show Z_{p^∞} is divisible.

Proof: True. It suffices to show $\mathbb{Z}_{p^\infty}$ is injective, and for this we show it is divisible as a $\mathbb{Z}$-module. Take any $m \in \mathbb{Z}$ such that $m \neq 0$; then we need to show for all $\frac{a}{p^i} + \mathbb{Z} \in \mathbb{Z}_{p^\infty}$ that there exists a $\frac{b}{p^j} + \mathbb{Z}$ such that

$$\frac{a}{p^i} \equiv m\frac{b}{p^j} \pmod{\mathbb{Z}}.$$

We begin with generators: Let $m = kp^l$ so that $(k,p) = 1$. As such we know there exists integers s and t such that: $sk + tp^i = 1$, equivalently: $p^i | sk - 1$, or

$$\frac{1}{p^i} \equiv \frac{sk}{p^i} \equiv m\frac{s}{p^{i+l}} \pmod{\mathbb{Z}}.$$

Thus each generator is divisible, but this is temporary for certainly then:

$$\frac{a}{p^i} \equiv m\frac{as}{p^{i+l}} \pmod{\mathbb{Z}},$$

and so in fact $\mathbb{Z}_{p^\infty}$ is divisible. □

Hint: Show $\mathbb{Q}[x, x^{-1}]$ is not free.

108 Projectives over PIDs – True or False? $\mathbb{Q}[x, x^{-1}]$ is a projective $\mathbb{Q}[x]$-module.

Proof: $\mathbb{Q}[x, x^{-1}]$ will be projective only if it is a free $\mathbb{Q}[x]$-module, since $\mathbb{Q}[x]$ is a PID. Clearly any basis must be of size 2 or greater. If we select any two elements from $\mathbb{Q}[x, x^{-1}]$, $q = \sum_{i=-k}^{l} q_i x^i$ and $p = \sum_{i=-m}^{n} p_i x^i$ then $x^k q, x^m p \in \mathbb{Q}[x]$ so we have $a = x^m p x^k$ and $b = x^k q x^m$ both in $\mathbb{Q}[x]$ and also

$$((x^m p)x^k)q - ((x^k q)x^m)p = x^m p x^k q - x^m p x^k q = 0.$$

Therefore any two elements of $\mathbb{Q}[x, x^{-1}]$ are $\mathbb{Q}[x]$-linearly dependent so that $\mathbb{Q}[x, x^{-1}]$ has no basis and is not free. □

Hint: Notice that R is projective so it is a direct summand of W and W'.

109 Module Quotients Let R be a ring and $V \leq W$, $V' \leq W'$ be R-modules such that $W/V \cong R \cong W'/V'$ and $V \cong V'$ then $W \cong W'$.

Proof: Since R is projective it follows every short exact sequence that ends in R splits. Thus

$$\mathbf{0} \longrightarrow V \longrightarrow W \longrightarrow R \longrightarrow \mathbf{0}$$

and

$$\mathbf{0} \longrightarrow V' \longrightarrow W' \longrightarrow R \longrightarrow \mathbf{0}$$

split, so indeed $W = V \oplus R$ and $W' \cong V' \oplus R$. But $V \cong V'$ so $W \cong W'$.[11] □

Hint: Use Baer's Criterion.

110 Injectivity of Fraction Fields Let R be an integral domain and F its field of fractions. Prove that F is an injective R-module.

Proof: We make use of Baer's Criterion. So consider the following diagram, $I \trianglelefteq R$:

$$\begin{tikzcd} & {}_R F & \\ \mathbf{0} \arrow[r] & {}_R I \arrow[u, "f"] \arrow[r, "i"] & {}_R R \arrow[ul, dashed, "g"'] \end{tikzcd}$$

[11]A truly convincing proof here uses the 5-lemma on the short exact sequence with the middle map defined by the split map from W to V, followed by the isomorphism of V to V' followed by the inclusion of V' to W'.

Given non-zero values $a, b \in I$ it is clear by linearity that

$$af(b) = f(ab) = f(ba) = bf(a); \qquad f(a)/a = f(b)/b = c.$$

Define $g(r) = rc$ and clearly for any non-zero $a \in I$ it follows $g(a) = af(a)/a = f(a)$, so g extends f.[12] Moreover, $g(sx + y) = sxc + yc = sg(x) + g(y)$ so it is R-linear. Hence g extends f so by Baer's Criterion F is injective as and R-module. $\square$

111 Injective Hulls – True or False? $\mathbb{Q}$ is the injective hull of $\mathbb{Z}$.

Hint:

Definition 3.0.12 *Given R-modules $X \leq Q$, and Q', with Q and Q' injective R-modules, then Q is an injective hull (injective envelope) of X if given any monomorphism $g : X \to Q'$ there exists a monomorphism $h : Q \to Q'$ so that the following diagram commutes:*

$$\begin{tikzcd} & 0 \arrow[d] & \\ 0 \arrow[r] & X \arrow[r, "i"] \arrow[d, "g"'] & Q \arrow[dl, dashed, "h"'] \\ & Q' & \end{tikzcd}$$

Proof: True. We see $\mathbb{Q}$ is divisible as $n\mathbb{Q} = \mathbb{Q}$ for any $n \in \mathbb{Z}$, $n \neq 0$. Clearly $\mathbb{Z} \leq \mathbb{Q}$. Now take any other injective module Q' with $\mathbb{Z}$ embedded via a map $g : \mathbb{Z} \to Q'$. As Q' is injective over $\mathbb{Z}$ it is divisible by $\mathbb{Z}$. So $nQ' = Q'$ for any n.

Take $1 \in Q'$ to be the element $g(1)$. Then for all $b \in \mathbb{Z}$, $b \neq 0$, $bQ' = Q'$ so there exists an element $c \in Q'$ such that $bc = 1$. Now suppose $c' \in Q'$ also has the property that $bc' = 1$. Then $bc = bc'$ and so $b(c - c') = 0$. Let $x = c - c'$. If $x = 0$ we are done. If $x \neq 0$ then $bx = 0$ tells us there must be a $y \in Q'$ such that $bx_1 = x$. But then $b^2x_1 = 0$ and we repeat. In the end $b^{n+1}x_n = 0$ for all n so in the end x_∞ has no $y \in \mathbb{Q}$ such that $by \neq x_\infty$ as then $b^2y = 0$. in Q' then Thus given any $a/b \in \mathbb{Q}$, there exists a $c \in Q'$ such that $bc = g(a)$. Define $h : \mathbb{Q} \to Q'$ as $h(a/b) = c$. Suppose that $c' \in Q'$ also has the property that $bc' = g(a)$. Then

As $(b, 1) = 1$, there are integers n, m such that $1 = mb + n1$ $\square$

112 Semi-simple Modules Every short exact sequence of $\mathbb{C}[x]/(x^2 - 1)$-modules splits.

Hint: Show that the ring is semi-simple artinian.

Proof: It is sufficient to show that $\mathbb{C}[x]/(x^2 - 1)$ is semi-simple artinian; for then every module is injective and projective, and so every short exact sequence splits. Let $I = (x^2 - 1)$. Notice that the only proper ideals are $((x - 1) + I)$ and $((x + 1) + I)$. This intersect trivially, and their sum is the entire ring, thus $\mathbb{C}[x]/(x^2 - 1)$ has a complement for every submodule over itself, so it is semi-simple artinian. $\square$

113 Semi-simple Modules – True or False? Every short exact sequence over $\mathbb{Z}_{15}$-modules splits.

Hint: Show that $\mathbb{Z}_{15}$ is semi-simple artinian.

Proof: True. Notice $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$ which is the form of the Wedderburn-Artin theorem, so $\mathbb{Z}_{15}$ is semi-simple artinian. Hence, every module is projective and

[12] Assume that R is canonically embedded in F already so that rc is well-defined.

injective, so every short exact sequence splits. □

Hint: Show $\mathbb{R}[x]$ is not artinian.

114 Projective $\mathbb{R}[x]$-modules – True or False? Every $\mathbb{R}[x]$-module is projective.

Example: False. If every module is projective, then every short exact sequence splits, and consequently every module is also injective. This shows every submodule has a complement, so every module is semi-simple. But this is a condition equivalent to requiring that $\mathbb{R}[x]$ be semi-simple artinian. Thus if $\mathbb{R}[x]$ is not, then some submodule is not projective. Clearly the chain

$$(1) \geq (x) \geq (x^2) \geq \cdots$$

is an infinite descending, never stabilizing, chain, so $\mathbb{R}[x]$ is not artinian. □

Hint: Consider any ring product ring.

115 Projectivity and Freeness – True or False? Every projective module over a commutative ring is free.

Example: False. Let the ring be $R = \mathbb{Z}/2 \oplus \mathbb{Z}/2$. If we define $\mathbb{Z}/2$ as a left $\mathbb{Z}/2 \oplus \mathbb{Z}/2$-module by noticing $I = ((1,0))$ is a left ideal of R. Moreover, $J = ((0,1))$ is also a left-ideal and $I \oplus J = R$ so I is a direct summand of R. Yet I has order 2, not a multiple of 4, so it cannot be a free R-module, yet it is still projective. □

Hint: Map a basis $\{e_i\}$ to $\{\varepsilon_i\}$ where $\varepsilon_i(e_j) = \delta_{ij}$ – the Kronecker delta.

116 Dual Modules Let F be a free left R-module with finite basis. Prove that F^* is a free right R-module with finite basis dual to the basis of F. Prove that F is reflexive.

Proof: Let $e_1, \ldots, e_n$ be a basis for F. Define the linearly functionals $\varepsilon_i(e_j) = \delta_{ij}$ and extend ϵ_i by linearization. Define the map E from $_RF$ to $F_R^* = Hom_R(_RF,_R R_R)$ as $e_i \mapsto \epsilon_i$ and generalize by linearization as follows:

$$\sum_{i=1}^{n} \lambda_i e_i \mapsto \sum_{i=1}^{n} \varepsilon_i l_i.$$

The map is clearly well-defined and R-linearly. Now take any $f \in F^*$. It follows

$$f(x) = f\left(\sum_{i=1}^{n} \lambda_i e_i\right) = \sum_{i=1}^{n} \lambda_i f(e_i) = \sum_{i=1}^{n} \lambda_i f_i \varepsilon_i(e_i) = \sum_{i=1}^{n} f_i \sum_{i=1}^{n} \varepsilon_i(\lambda_i e_i) = \sum_{i=1}^{n} f_i \varepsilon_i(x).$$

Therefore $f = f_1\varepsilon_1 + \cdots + f_n\varepsilon_n$ and so $\varepsilon_1, \ldots, \varepsilon_n$ is a basis of F_R^*. So not only is F_R^* finite dimensional, it has the same dimension as F; thus by the universal property of free modules, $F \cong F^*$ as they are free on cardinally equivalent bases. Hence $F \cong F^{**}$ proving F is reflexive. □

Hint: Use the fact that P is a direct summand of a free module and the already proven result for free modules – see Exercise-3.116.

117 Duals of Projectives Let P be a finitely generated projective R-module. Prove that P^* is a finitely generated projective right R-module, and that P is reflexive. Demonstrate that both statements may be false if P is not finitely generated.

Proof: Let $\{v_1, \ldots, v_n\}$ be a set of generators for P. We may define the Kronecker $\delta_{i,j}$ maps as $\delta_{i,j} = 0$ when $i \neq j$ and 1 when $i = j$. From this we may define the maps $f_i : P \to R$ by $f_i(v_j) = \delta_{i,j}$, and generalized linearly. These maps lie in $P^* = Hom_R(_RP,_R R_R)$, which is a right R-module. Furthermore, as P is generated by $\{v_1, \ldots, v_n\}$ we may take any map $g \in P^*$ and express

$g = gf_1 + \cdots gf_n$. Thus P^* is finitely generated. Moreover, we may show $P^{**} \cong P$ with the following isomorphism:

$$\varphi : p \mapsto (\varphi_p : g \mapsto g(p)).$$

Suppose $\varphi_p = \varphi_q$. Then for all $g \in P^*$ it follows $g(p) = g(q)$. However, we know $f_i(v_i) = 1$ while $f_i(v_j) = 0$ for all $i \neq j$ so letting $g = f_i$ we see the requirement that $p = q$; thus the map is injective.

That φ is linear follows from the linearity in each component:

$$\varphi_{sp+q}(g) = g(sp+q) = sg(p) + g(q) = s\varphi_p(g) + \varphi_q(g).$$

All that remains is surjectivity. Recall that P^* is generated by $\{f_1, \dots, f_n\}$. Now take any $\psi \in P^{**}$. Clearly

$$\psi(r_1v_1 + \cdots + r_nv_n) = r_1\psi(v_1) + \cdots + r_n\psi(v_n).$$

Now provided $\psi(v_1), \dots, \psi(v_n)$ generate P^{**} we are done. But certainly this is true because each $\psi(v_i)(f_j) = \delta_{i,j} = g_i(f_j)$, where $\{g_i\}$ is a basis for P^{**}. (Notice the size of the generating sets in P, P^*, and P^{**} are all equal.)

To show P^* is projective consider the characterization of projective modules as a direct summand of a free module. Recall that

$$Hom_R\left(\bigoplus_{i=1}^n {}_RR_R, {}_RR_R\right) = \prod_{i=1}^n Hom_R({}_RR_R, {}_RR_R) = \prod_{i=1}^n {}_RR_R = \bigoplus_{i=1}^n {}_RR_R.$$

Moreover, P is finitely generated so it is a direct summand of a finitely generated free R-module (consult the proof of the characterization to verify finiteness is implied.) Finally, $Hom_R(-, {}_RR_R)$ takes split exact sequences to split exact sequences, so we obtain:

$$\begin{tikzcd}
\mathbf{0} \arrow[r] & P \arrow[r] \arrow[d, "Hom(-,R)"] & \bigoplus_{i=1}^n {}_RR_R \arrow[r] \arrow[d, "Hom(-,R)"] & Q \arrow[r] \arrow[d, "Hom(-,R)"] & \mathbf{0} \\
\mathbf{0} \arrow[r] & P^* \arrow[r] & \bigoplus_{i=1}^n {}_RR_R \arrow[r] & Q^* \arrow[r] & \mathbf{0}
\end{tikzcd}$$

Since we now see P^* is a direct summand of a free R-module it is clear that P^* is projective. $\square$

Example: If we let $P = \bigoplus_{\mathbb{N}} \mathbb{F}_2$ then it is projective as it is a module in the category of semi-simple artinian ring. However P^{**} has cardinality $2^{\aleph_0} > \aleph_0$ so P is not isomorphic to P^{**}. So P is not reflexive.

Now suppose $P = \bigoplus_{\mathbb{N}} \mathbb{Z}$. As coproducts of projectives are projective we know P is projective. However, once again, P^* is $\prod_{\mathbb{N}} \mathbb{Z}$ which is not projective as it is not a direct summand of a free module. $\square$

118 Finite Dimensional Duals Let V be a finite dimensional vector space over a division ring D. Prove that V is reflexive.

Hint: Use Exercise-3.116.

Proof: Since V is a vector space it is a free module. Thus V^* is a free module of the same rank (Exercise-3.116) and so $V \cong V^{**}$. $\square$

119 Projectivity and Fields Prove that a domain R is a field if and only if every R-module is projective.

Hint: Use the Wedderburn-Artin theorem to characterize R.

Proof: Let R be an integral domain.

Suppose that every R-module is projective. Then every short exact sequence splits so every module is semi-simple. Thus R is semi-simple artinian. Applying Wedderburn-Artin we see

$$R \cong M_{n_1}(D_1) \oplus \cdots M_{n_k}(D_k).$$

Yet $k = 1$ or otherwise the decomposition reveals zero-divisors, for instance $I_{n_1} \oplus 0 \cdots \oplus 0$ and $0 \oplus \cdots \oplus 0 \oplus I_{n_k}$. Also R is commutative so $n_1 = 1$ and D_1 is commutative. Therefore R is the field D_1.

Now suppose that R is a field. Then R is semi-simple artinian so every short exact sequence splits. In particular every module is projective. □

Hint: Use the middle linear property of tensors.

120 Subring Tensors Let R be a subring of the ring S such that S is a free right R-module with basis $\{s_i : i \in I\}$. If V is a left R-module, then, as abelian groups,

$$S \otimes_R V = \bigoplus_{i \in I} s_i \otimes V,$$

where $s_i \otimes V$ denotes the subspace of $S \otimes_R V$ generated by all pure tensors of the form $s_i \otimes v$.

Proof: Recall the submodule generated by each s_i is $s_i R$. So indeed we have:

$$S \otimes_R V = \left(\bigoplus_{i \in I} s_i R \right) \otimes V = \bigoplus_{i \in I} s_i R \otimes V = \bigoplus s_i \otimes V,$$

where we observe that any element $s_i r \otimes v$ can be written as $s_i \otimes rv$ and thus fits our given form. □

Hint: Use the universal property of tensors to construct the maps. Do not forget to invert each for the isomorphism.

121 Tensors over PIDs Let V and W be $\mathbb{Z}$-modules.

(i) $V \otimes \mathbb{Z}/m\mathbb{Z} \cong V/mV$.

(ii) $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z}$ where $k = (m, n)$.

(iii) Describe $V \otimes W$ if V and W are finitely generated.

Proof:

(i) Define the map $f : V \times \mathbb{Z}/m\mathbb{Z} \to V/mV$ by $(v, \overline{k}) = kv$. Given any $k \equiv j \pmod{m}$ if follows $k - j = l \cdot m$ so that indeed

$$(kv + mV) - (jv + mV) = (k - j)v + mV = l \cdot mv + mV = mV;$$

therefore, $kv \equiv jv \pmod{mV}$, and f is well-defined. Also

$$f(rv, \overline{k}) = krv = rkv = f(v, r\overline{k})$$

for all $r \in \mathbb{Z}$. Finally:

$$f(v + w, \overline{k}) = kv + kw = f(v, \overline{k}) + f(w, \overline{k})$$

and

$$f(v, \overline{k} + \overline{j}) = kv + jv = f(v, \overline{k}) + f(v, \overline{j});$$

hence, f is $\mathbb{Z}$-balanced and so by the universal property of tensors there exists a $\mathbb{Z}$-balanced map (furthermore a group homomorphism as $\mathbb{Z}$ is commutative so the tensor product is again a $\mathbb{Z}$-module and the induced maps $\mathbb{Z}$-homomorphisms): $\tilde{f} : V \otimes \mathbb{Z}/m\mathbb{Z} \to V/mV$ which covers f.

Now define its inverse as: $g : V/mV \to V \otimes \mathbb{Z}/mZ$ by $g(v + mV) = v \otimes \overline{1}$. Clearly

$$\tilde{f}(g(v + mV)) = \tilde{f}(v \otimes \overline{1}) = f(v, \overline{1}) = 1v + mV = v + mV.$$

Also

$$g(\tilde{f}(v \otimes \overline{k})) = g(f(v, \overline{k})) = g(kv + mV) = kv \otimes \overline{1} = v \otimes \overline{k}.$$

Thus g and f are indeed inverses and so f is a bijective $\mathbb{Z}$-homomorphism and thus a module isomorphism.

(ii) Let $V = \mathbb{Z}/m\mathbb{Z}$. From part (i) we see that $V \otimes \mathbb{Z}/n\mathbb{Z} = V/nV$ so in our situation we have $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z})/m(\mathbb{Z}/n\mathbb{Z})$. However, this is nothing more than $\mathbb{Z}/(m, n)\mathbb{Z}$.

(iii) If V and W are finitely generated we may decompose them as:

$$V \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z}; \qquad W \cong \mathbb{Z}/e_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_l\mathbb{Z},$$

where $d_1|d_2|\cdots|d_k$, and $e_1|\cdots|e_l$ and we allow d_i and e_i to be 0 if free parts appear. By distributing and using part (ii) we see:

$$\begin{aligned} V \otimes W &\cong (\mathbb{Z}/d_1\mathbb{Z} \otimes W) \oplus \cdots \oplus (\mathbb{Z}/d_k\mathbb{Z} \otimes W) \\ &\cong (\mathbb{Z}/d_1\mathbb{Z} \otimes \mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_1\mathbb{Z} \otimes \mathbb{Z}/e_l\mathbb{Z}) \\ &\qquad \vdots \\ &\quad \oplus (\mathbb{Z}/d_k\mathbb{Z} \otimes \mathbb{Z}/e_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_k\mathbb{Z} \otimes \mathbb{Z}/e_l\mathbb{Z}) \\ &\cong \bigoplus_{i=1,j=1}^{k,l} \mathbb{Z}/(d_i, e_j)\mathbb{Z}. \end{aligned}$$

□

122 Torsion and Tensors – True or False? If V is a torsion module over R a PID and Q any field containing R. Then $V \otimes Q = 0$.

Hint: Pull across the the pure tensors, any annihilator of any torsion elements.

Proof: True. Given any element $a \in V$, let (p) be the order ideal of a. Since V is a torsion module over a PID, we know $p \neq 0$. Thus p^{-1} exists in Q. Furthermore we now see given any pure tensor $q \otimes a$ we have:

$$q \otimes a = \frac{q}{p} p \otimes a = \frac{q}{p} \otimes pa = \frac{q}{p} \otimes 0 = 0.$$

As every pure tensor is 0, the entire group is trivial. □

123 Fraction Field Tensors – True or False? $\mathbb{Q} \otimes \mathbb{Q} \cong \mathbb{Q}$?

Hint: Normalize one component of each pure tensor.

Proof: True. Define $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ by $f(q, p) = qp$. Since products in $\mathbb{Q}$ are well-defined, so is this map. Now take any $r \in \mathbb{Z}$, certainly

$$f(qr, p) = qrp = f(q, rp)$$

and $s \in \mathbb{Q}$ also yields:

$$f(s+q, p) = sp+qp = f(s, p)+f(q, p); \qquad f(q, s+p) = qs+qp = f(q, s)+f(q, p).$$

Therefore, f is $\mathbb{Z}$-balanced so it induces a $\mathbb{Z}$-balanced (and furthermore, $\mathbb{Z}$-linear), map $\tilde{f} : \mathbb{Q} \otimes \mathbb{Q} \to \mathbb{Q}$. Now we must simply invert the map.

Take $g : \mathbb{Q} \to \mathbb{Q} \otimes \mathbb{Q}$ by $g(q) = q \otimes 1$. Clearly this map is well-defined and now we check it is an inverse:

$$\tilde{f}(g(q)) = \tilde{f}(q \otimes 1) = f(q, 1) = q \cdot 1 = q.$$

$$g(\tilde{f}(q \otimes p)) = g(f(q, p)) = g(qp) = qp \otimes 1.$$

Now we must show that $q \otimes p = qp \otimes 1$. To begin with notice $m(p \otimes q) = 0$ implies $mp = 0$ or $mq = 0$. But assuming $p \otimes q \neq 0$ then $q \neq 0$ and $q \neq$ so $mp \neq 0$ and $mq \neq 0$ unless $m = 0$ – we have a torsion free module. Now notice:

$$bd\left(\frac{a}{b}\frac{c}{d} \otimes 1\right) = ac \otimes 1 = a \otimes c$$

and

$$bd\left(\frac{a}{b} \otimes \frac{c}{d}\right) = a \otimes c;$$

therefore,

$$bd\left(\frac{a}{b}\frac{c}{d} \otimes 1 - \frac{a}{b} \otimes \frac{b}{c}\right) = 0.$$

Sense we have a torsion free module this means we have:

$$pq \otimes 1 = \frac{a}{b}\frac{c}{d} \otimes 1 = \frac{a}{b} \otimes \frac{c}{d} = p \otimes q.$$

Thus f and g are inverse maps, and f is a homomorphism, so f is an isomorphism. □

Hint: Both are false.

124 Tensor Isomorphisms – True or False? Let V be a right R-module and W be a left R-module. True or False?

(i) There is an isomorphism of abelian groups $V \otimes_R W \cong V \otimes_{\mathbb{Z}} W$?

(ii) If $v \otimes w = v' \otimes w'$ in $V \otimes_R W$, then $v = v'$ and $w = w'$.

Example: Both are false. For (i) consider letting $R = \mathbb{Z} \oplus \mathbb{Z}$. Then

$$\mathbb{Z} \oplus_{\mathbb{Z}\oplus\mathbb{Z}} \mathbb{Z} \oplus \mathbb{Z} = \mathbb{Z}; \qquad \mathbb{Z} \oplus_{\mathbb{Z}} \mathbb{Z} \oplus \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}.$$

For (ii) consider $2 \otimes 3 = 1 \otimes 6$ in $\mathbb{Z} \otimes \mathbb{Z}$. Certainly $2 \neq 1$ and $3 \neq 6$. □

Hint: Use the universal property in both directions.

125 Tensors and Quotients If V' is a submodule of the right R-module V and W' is a submodule of the left R-module W, then $(V/V') \otimes_R (W/W') \cong (V \otimes_R W)/U$, where U is the subgroup of $V \otimes_R W$ generated by all elements of the form $v' \otimes w$ and $v \otimes w'$ with $v' \in V'$ and $w \in W$, and $v \in V$ and $w' \in W$.

Proof: Declare $g : V \times W \to V/V' \otimes W/W'$ by $g(v, w) = (V' + v) \oplus (w + W')$. First our map is well-defined as the cosets lie in the image not the domain. Next we must verify this map is R-balanced:

$$\begin{aligned}
g(vr, w) &= (V' + vr) \otimes (w + W') = (V' + v) \otimes (rw + W') = g(v, rw);\\
g(v + u, w) &= V' + (v + u) \times w + W'\\
&= ((V' + v) \otimes (w + W')) + ((V' + u) \otimes (w + W'))\\
&= g(v, w) + g(u, w);\\
g(v, w + u) &= (V' + v) \times ((w + u) + W')\\
&= ((V' + v) \otimes (w + W')) + ((V' + u) \otimes (u + W'))\\
&= g(v, w) + g(v, u).
\end{aligned}$$

As g is R-balanced it induces an R-balanced map $\overline{g} : V \otimes W \to V/V' \otimes W/W'$. Furthermore, on pure tensors alone $\overline{g}$ is surjective, thus we need only look for its kernel to establish an isomorphism.

Notice indeed given any $v' \in V'$ and any $w \in W$ that

$$\overline{g}(v' \otimes w) = g(v', w) = (V' + v') \otimes (w + W') = 0 \otimes (w + W') = 0.$$

Likewise given $w' \in W'$ and $v \in V$ we have $\overline{g}(v \otimes w') = 0$. Therefore U is contained in the kernel of $\overline{g}$. Thus we have g factors through U so we may abusively write:

$$\overline{g} : V \oplus W/U \to V/V' \otimes W/W'.$$

Now we look to construct an inverse map.

Notice $U = V' \otimes W + V \otimes W'$ and declare $f : V/V' \times W/W' \to V \otimes W/U$ by

$$f(V' + v, w + W') = v \otimes w + U.$$

First we must verify the f is well-defined. Given $V' + v = V' + u$ and $w + W' = x + W'$ we see $v - u \in V'$ and $w - x \in W'$ so:

$$f(V' + (v - u), (w - x) + V') = (v - u) \otimes (w - x) + U = U;$$

therefore, f is well-defined. Moreover f is middle linear:

$$\begin{aligned}
f(V' + vr, w + W') &= vr \otimes w + U = v \otimes rw + U; \\
f((V' + v) + (V' + u), w + W') &= f(V + (v + u), w + W') = (v + u) \otimes w + U \\
&= (v \otimes w + U) + (u \otimes w) + U = f(V' + v, w + W') + f(V' + u, w + W'); \\
f(V' + v, (w + W') + (x + W')) &= f(V' + v, (w + x) + W') = v \otimes (w + x) + U \\
&= (v \otimes w + U) + (v \otimes x + U) = f(V' + v, w + W') + f(V' + v, x + W').
\end{aligned}$$

Therefore we have an induced map on the tensor which visibly is the inverse of $\overline{g}$. Therefore we have an isomorphism of groups. $\square$

126 Tensors of Exact Sequences If

$$\mathbf{0} \longrightarrow A \xrightarrow{f} C \xrightarrow{g} B \longrightarrow \mathbf{0}$$

is split exact sequence of left R-modules, then

$$\mathbf{0} \longrightarrow X \otimes_R A \xrightarrow{id_X \otimes f} X \otimes_R C \xrightarrow{id_X \otimes g} B \longrightarrow \mathbf{0}$$

is an exact sequence of abelian groups for any right R-module X.

Hint: Use the split to distribute the tensor then consider the components of the sequence.

Proof: Since our given sequence splits it follows $C \cong A \oplus B$ so we may consider instead the following diagram:

$$\begin{tikzcd}
& & A \arrow[d, shift right, "\iota_A"'] \arrow[dr, "0"] & & \\
\mathbf{0} \arrow[r] & A \arrow[ur, "1_A"] \arrow[r, "g"] \arrow[dr, "0"'] & C \arrow[u, shift right, "\pi_A"'] \arrow[r, "f"] \arrow[d, shift right, "\pi_B"'] & B \arrow[r] & \mathbf{0} \\
& & B \arrow[u, shift right, "\iota_B"'] \arrow[ur, "1_B"'] & &
\end{tikzcd}$$

Now we tensor with X and notice that

$$X \otimes C \cong X \otimes (A \oplus B) = (X \otimes A) \oplus (X \otimes B).$$

Moreover, this sequence splits naturally. Thus we see componentwise the above sequence with tensors is exact. Specifically we have the following natural construction:

$$\begin{tikzcd}
 & & X\otimes A \arrow[d, shift right, "1_X\otimes\iota_A"'] \arrow[drr, "0"] & & \\
\mathbf{0} \arrow[r] & X\otimes A \arrow[ur, "1_X\otimes 1_A"] \arrow[r, "1_X\otimes g"] \arrow[dr, "0"'] & X\otimes C \arrow[u, shift right, "1_x\otimes\pi_A"'] \arrow[r, "1_X\otimes f"] \arrow[d, shift right, "1_X\otimes\pi_B"'] & X\otimes B \arrow[r] & \mathbf{0}. \\
 & & X\otimes B \arrow[u, shift right, "1_X\otimes\iota_B"'] \arrow[ur, "1_X\otimes 1_B"'] & &
\end{tikzcd}$$

□

Hint: Use the fact that projectives are direct summands of free modules and the visible fact that free modules are flat.

127 Flat Modules

Prove that a projective module is flat.

Proof: Given a projective module P there exists a module Q such that $F = P\oplus Q$ is a free R-module. A free module is isomorphic to $\bigoplus R$ for some index set so we observe given any module A that $F\otimes A\cong\bigoplus A$. Thus given a short exact sequence:

$$\mathbf{0}\longrightarrow A\xrightarrow{f} B\xrightarrow{g} C\longrightarrow\mathbf{0}$$

it follows:

$$\mathbf{0}\longrightarrow F\otimes A\xrightarrow{1\otimes f} F\otimes B\xrightarrow{1\otimes g} F\otimes C\longrightarrow\mathbf{0}$$

is short exact as it is componentwise, and each element in the sequence is a coproduct (universal property of coproducts infers the exactness on the entire coproduct.) But now we translate the information using $F = P\otimes Q$:

$$\begin{tikzcd}
\mathbf{0} \arrow[r] & (P\otimes A)\oplus(Q\otimes A) \arrow[r, "1\otimes f\oplus 1\otimes f"] \arrow[d, "\pi_A"] & (P\otimes B)\oplus(Q\otimes B) \arrow[r, "1\otimes g\oplus 1\otimes g"] \arrow[d, "\pi_B"] & (P\otimes C)\oplus(Q\otimes C) \arrow[r] \arrow[d, "\pi_C"] & \mathbf{0} \\
\mathbf{0} \arrow[r] & P\otimes A \arrow[r, "1\otimes f"] & P\otimes B \arrow[r, "1\otimes g"] & P\otimes C \arrow[r] & \mathbf{0},
\end{tikzcd}$$

where π_A is the projection along $Q\otimes A$ to $P\otimes A$, etc. As these projections are surjective we see the diagram commutes. Now we will use the exactness of the first row to deduce the exactness of the second row – we diagram chase.

Take $a\in Ker\ 1\otimes f$. Since π_A is epic, there exists a $a'\oplus a''$ which maps to a via π_A. Likewise, there exists a $0\oplus b$ in the pre-image of 0 via π_B since it is projection to $P\otimes B$ along $Q\otimes B$. Since the diagram commutes we see:

$$\begin{tikzcd}
a'\oplus a'' \arrow[r, mapsto, "(1\otimes f)\oplus(1\otimes f)"] \arrow[d, mapsto] & 0\oplus b \arrow[d, mapsto] \\
a \arrow[r, mapsto, "1\otimes f"] & 0
\end{tikzcd}$$

But $(1\otimes f)\oplus(1\otimes f)$ is monic so $a' = 0$ and so $a = 0$, and so $1\otimes f$ is monic.

Now take any $c\in P\otimes C$. Since π_C is surjective it follows there exists a $c'\oplus c''$ such that $\pi_C(c'\oplus c'') = c$. Recall that the top row is exact so $(1\otimes g)\oplus(1\otimes g)$ is epic and so there exist a $b'\oplus b''$ which covers $c'\oplus c''$. But now we simply project the element to b via π_B and as the diagram commutes we see b covers c:

$$\begin{tikzcd}
b'\oplus b'' \arrow[r, mapsto, "(1\otimes g)\oplus(1\otimes g)"] \arrow[d, mapsto] & c'\oplus c'' \arrow[d, mapsto] \\
b \arrow[r, mapsto, "1\otimes g"] & c
\end{tikzcd}$$

Now we must show the sequence is exact at B. So first is $Im\ 1 \otimes f \geq Ker\ 1 \otimes g$? Take any $b \in Ker\ 1 \otimes g$. Since this maps to 0 via $1 \otimes g$ we may pullback to 0 in $(P \otimes C) \oplus (Q \otimes C)$ with π_C. Next we use the exactness of the top row to assert the existence of b' which maps to b via π_B and to 0 via $(1 \otimes g) \oplus (1 \otimes g)$. Thus the exactness in the top row gives the existence of an a' that maps to b' and if we project this using π_A we get an a that maps to b which maps to 0. Therefore, every element in the $Ker\ 1 \otimes g$ is contained in the image of $1 \otimes f$.

$$\begin{tikzcd}
a' \arrow[r, mapsto, "5"] \arrow[d, mapsto, "6"] & b' \arrow[r, mapsto, "3"] \arrow[d, mapsto, "4"] & 0 \arrow[d, mapsto, "2"] \\
a \arrow[r, mapsto, "7"] & b \arrow[r, mapsto, "1"] & 0
\end{tikzcd}$$

Now take any $a \in P \otimes A$ and consider its image $b = (1 \otimes f)(a)$. This element we retract along π_B to some b' which intern we see is in the image of $(1 \otimes f) \oplus (1 \otimes f)$ by retracting a along π_A and using the commutativity of the square. Thus b' maps to 0 over the tensor of g, and so its projection also maps to 0 proving $Im\ 1 \otimes f \leq Ker\ 1 \otimes g$. Unfortunately the resulting diagram chase is identical and not enlightening:

$$\begin{tikzcd}
a' \arrow[r, mapsto, "3"] \arrow[d, mapsto, "4"] & b' \arrow[r, mapsto, "5"] \arrow[d, mapsto, "2"] & 0 \arrow[d, mapsto, "6"] \\
a \arrow[r, mapsto, "1"] & b \arrow[r, mapsto, "7"] & 0
\end{tikzcd}$$

In the end we agree the second row is exact and so indeed projective modules are flat. $\square$

128 Induced Quotient Modules

Hint: Use the universal property of tensors.

(i) If I is a right ideal of R and V is a left R-module, then there is an isomorphism of abelian groups

$$R/I \otimes_R V \cong V/IV,$$

where IV is the subgroup of V generated by all elements xv with $x \in I$, $v \in V$.

(ii) If R is a commutative and I, J are ideals in R, then $R/I \otimes_R R/J \cong R/(I + J)$.

Proof:

(i) Define the map $f : R/I \times_R V \to V/IV$ on the pure tensors as: $f(r + I, v) = rv + IV$. That f is well-defined follows from $r + I = s + I$ implies $rv - sv + IV = (r - s)v + IV = IV$. Moreover,

$$\begin{aligned}
f((r+I)s, v) &= f(rs + I, v) = rsv + IV = f(r + I, sv); \\
f((r+I) + (s+I), v) &= f((r+s) + I, v) = (rv + +IV) + (sv + IV) \\
&= f(r + I, v) + f(s + I, v); \\
f(r + I, v + w) &= (rv + IV) + (rw + IV) = f(r + I, v) + f(r + I, w).
\end{aligned}$$

Therefore f is R-balance so it induces a map $\overline{f}$ from the tensor to V/IV. Now we must build an inverse map and we will conclude this map is an isomorphism.

Take $g : V/IV \to R/I \otimes_R V$ to be $v + IV \mapsto (1 + I) \otimes v$, and of course generalize linearly. First take $v + IV = v' + IV$ so that $v - v = iw$ for some $w \in V$, and $i \in I$. Then

$$g(0) = g((v+IV)-(v'+IV)) = (1+I)\otimes v-v' = (1+I)\otimes iw = I\otimes w = 0.$$

Therefore g is well-defined. Now

$$\overline{f}(g(v + IV)) = \overline{f}((1 + I) \otimes v)) = f((1 + I) \otimes v) = v + IV.$$

Likewise

$$g(\overline{f}(((r+I)\otimes v)) = g(f((r+I)\otimes v)) = g(rv+IV) = (1+I)\otimes rv = (r+I)\otimes v.$$

So f is bijective so it is an isomorphism.

(ii) Consider $I(R/J)$. Given $i(r + J) = ir + iJ = i' + J$ where $i' = ir$ in I – which exists because I is an ideal, and J absorbs the i as well because it is an ideal. Therefore $I(R/J) \leq I + J/J$. Now let $r = 1$ and notice $i(1 + J) = i + J$ and so indeed $I + J/J \leq I(R/J)$ so $I + J/J = I(R/J)$. Now we notice by the third isomorphism theorem and our work in part (i) that:

$$R/I \otimes_R R/J \cong \frac{R/J}{I(R/J)} = \frac{R/J}{(I + J)/J} = R/(I + J).$$

□

Hint: Consider covering all pure tensors first.

129 Tensored Maps – True or False? If $f : V \to V'$ and $g : W \to W'$ are surjective maps of right and left R-modules respectively, then $f\otimes g$ is surjective.

Proof: True. Take a pure tensor $v' \otimes w' \in V' \otimes W'$. As f and g are surjective there exists a pure tensor $v \otimes w \in V \otimes W$ such that $f(v) \otimes g(w) = v' \otimes w'$. So $f \otimes g$ is surjective on pure tensors. However pure tensors generate $V' \otimes W'$ so $f \otimes g$ is surjective. □

Hint: Use the universal property of tensors to construct the maps.

130 Endomorphism Rings and Tensors Let R be a commutative ring and V and W be R-modules. Show that there exists a homomorphism of R-algebras

$$\theta : End_R(V) \otimes_R End_R(W) \to End_R(V \otimes W)$$

where

$$\theta(f \otimes g)(v \otimes w) = f(v) \otimes g(w),$$

for all $v \in V$, $w \in W$, $f \in End_R(V)$ and $g \in End_R(W)$.

Proof: First observe that both V and W are bi-modules so indeed ${}_RV_R \otimes_R W$ is an R-module and $End_R(V) = Hom_R({}_RV_{R,R}V)$ is an R-module as well as a ring, so indeed all objects concerned are R-algebras. Now we construct θ from the universal mapping property for tensors.

Let $\Theta : End_R(V) \times End_R(W) \to End_R(V \otimes W)$ be given by

$$\Theta(f, g) = f \otimes g.$$

As there are no equivalence classes we are assured this is well-defined and clearly $f \otimes g : V \otimes W \to V \otimes W \in End_R(V \otimes W)$. Now we check if Θ is middle linear.

$$\begin{aligned}
\Theta(f + h, g)(v \otimes w) &= ((f + h) \otimes g)(v \otimes w) = (f + h)(v) \otimes g(w) = f(v) + h(v) \otimes g(w) \\
&= f(v) \otimes g(w) + h(v) \otimes g(w) = (f \otimes g)(v \otimes w) + (h \otimes g)(v \otimes w) \\
&= ((f \otimes g) + (h \otimes g))(v \otimes w) = (\Theta(f, g) + \Theta(h, g))(v \otimes w); \\
\Theta(fr, g)(v \otimes w) &= (fr \otimes g)(v \otimes w) = f(v)r \otimes g(w) = f(v) \otimes rg(w) \\
&= (f \otimes rg)(v \otimes w) = \Theta(f \otimes rg)(v \otimes w).
\end{aligned}$$

Of course the sum in the right component is completely symmetric. Therefore Θ is middle linear so it induces the map θ which we see agrees with the stated definition. $\square$

131 Induced Modules over Tensors Suppose $f : R \to S$ is a surjective ring homomorphism. Let V and W be right and left S-modules respectively. Describe how to give V and W a right and left R-module structure and prove

$$V \otimes_R W \cong V \otimes_S W.$$

If f is not surjective, is $V \otimes_R W \cong V \otimes_S W$?

Hint: The obvious R-module structure is well-defined because of the partition induced by the surjection. Use the universal property of tensors for the rest.

Proof: Let $r \in R$ and $v \in V$, $w \in W$. Then define $r \cdot v = f(r)v$ and $r \cdot w = f(r)w$. Since $f(r) \in S$ it is clear that the extension to R is well-defined. To verify this is an R-module notice:

$$\begin{aligned} (r+s)\cdot v &= f(r+s)v = f(r)v + f(s)v = r\cdot v + s\cdot v; \\ (rs)\cdot v &= (f(r)f(s))v = r\cdot(f(s)v) = r\cdot(s\cdot v); \\ r\cdot(v+v') &= f(r)(v+v') = f(r)v + f(r)v' = r\cdot v + r\cdot v'. \end{aligned}$$

Now we construct the isomorphism by using the universal property of tensors. Let $g : V \times W \to V \otimes_S W$ be given by $g(v, w) = v \otimes w$. Given any $r \in R$ we have:

$$\begin{aligned} g(vr, w) &= vf(r) \otimes w = v \otimes f(r)w = g(v, rw) \\ g(v+u, w) &= (v+u) \otimes w = v \otimes w + u \otimes w = g(v, w) + g(u, w). \end{aligned}$$

Therefore we have an induced map $\overline{g} : V \otimes_R W \to V \otimes_S W$. For the reverse map we again use the universal property, but the design is a canonical embedding so the R-balance is clear: $\overline{h}(v \otimes w) = v \otimes w$. Clearly the two maps are inverses and so they are an isomorphism of abelian groups. $\square$

Example: No. Let $R = \mathbb{Z}$ and $S = \mathbb{Z} \oplus \mathbb{Z}$ with f the inclusion map $1 \mapsto (1, 0)$. Recall

$$Z \cong Z \otimes_{\mathbb{Z}\oplus\mathbb{Z}} \mathbb{Z} \oplus \mathbb{Z} \ncong Z \otimes_{\mathbb{Z}} \mathbb{Z} \oplus \mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}.$$

$\square$

132 Dimension and Tensors – True or False? If V and W are respectively right and left D-modules, for a division algebra D, such that $V \otimes_D W = \mathbf{0}$, then either $V = \mathbf{0}$ or $W = \mathbf{0}$.

Hint: $dim_D A \otimes B = dim_D A dim_D B$.

Proof: True. First recall that modules over a division ring are vector spaces, and as such are free and have well-defined dimension. Also recall

$$dim_D(V \otimes_D W) = dim_D V \cdot dim_D W$$

even if we consider infinite cardinalities (here 0 times infinity is 0.) Hence

$$0 = dim_D \mathbf{0} = dim_D V \otimes_D W = dim_D V \cdot dim_D W$$

which implies $dim_D V = 0$ or $dim_D W = 0$. Since vector spaces are free, this implies one of the two modules is trivial. $\square$

133 Annihilating Modules – True or False? Let R be a commutative ring and V be an R-module. If $L \otimes_R V = \mathbf{0}$ for every simple R-module L then $V = 0$.

Hint: Consider the case when all simple modules are torsion modules.

Example: False. Consider $R = \mathbb{Z}$ and $V = \mathbb{Q}$. We know each simple R-module to be $\mathbb{Z}/p$ for some prime p. However

$$\mathbb{Z}/p \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbf{0}.$$

But clearly $\mathbb{Q} \neq \mathbf{0}$. $\square$

Hint: Consider letting $X = R$.

134 Identity Tensor – True or False? Let V be a left R-module. If

$$X \otimes_R V \cong \mathbf{0}$$

for all right R-modules X, then $V \cong \mathbf{0}$.

Proof: True. Let $X = R_R$. Then we have two results which in the end prove our question:

$$\mathbf{0} \cong R_R \otimes_R V \cong V.$$

$\square$

Hint: Tensors distribute over the components of free modules, so a rank formula exists.

135 Tensors over Free Modules – True or False? If V, V_1, and V_2 are non-trivial free R-modules over a commutative ring R, where each is finitely generated and $V \otimes_R V_1 \cong V \otimes_R V_2$ then $V_1 \cong V_2$.

Proof: True. Notice that

$$rank_R V \cdot rank_R V_2 = rank_R V \otimes_R V_1 = rank_R V \otimes_R V_2 = rank_R V \cdot rank_R V_2.$$

As every term is finite, and non-zero, it follows by cancellation in the integers that $rank_R V_1 = rank_R V_2$. Any two free modules of the same rank are isomorphic, so $V_1 \cong V_2$. $\square$

Hint: Use Exercise-3.121.

136 Applied Tensors – True or False? $\mathbb{Z}_3 \otimes_{\mathbb{Z}} (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2) \cong \mathbb{Z}_6$.

Example: False.

$$\mathbb{Z}_3 \otimes_{\mathbb{Z}} (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2) \cong \mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong 0.$$

$\square$

Hint: Use Exercise-3.121.

137 Applied Tensors – True or False? Find $(\mathbb{Q} \oplus \mathbb{Z}_7) \otimes_{\mathbb{Z}} \mathbb{Z}_5$.

Example:

$$(\mathbb{Q} \oplus \mathbb{Z}_7) \otimes_{\mathbb{Z}} \mathbb{Z}_5 \cong (\mathbb{Q} \otimes \mathbb{Z}_5) \oplus (\mathbb{Z}_7 \oplus \mathbb{Z}_5) = \mathbf{0}.$$

$\square$

Hint: Use Exercise-3.121.

138 Applied Tensors – True or False? True or False: $\mathbb{Z}_{35} \otimes_{\mathbb{Z}} \mathbb{Z}_5 \cong \mathbb{Z}_7$?

Example: False.

$$\mathbb{Z}_{35} \otimes_{\mathbb{Z}} \mathbb{Z}_5 \cong \mathbb{Z}_5.$$

$\square$

Hint: Use Exercise-3.121.

139 Applied Tensors – True or False? Find $(\mathbb{C} \oplus \mathbb{Z}_6) \otimes_{\mathbb{Z}} \mathbb{Z}_3$.

Example:

$$(\mathbb{C} \oplus \mathbb{Z}_6) \otimes_{\mathbb{Z}} \mathbb{Z}_3 \cong (\mathbb{C} \otimes \mathbb{Z}_3) \oplus (\mathbb{Z}_6 \oplus \mathbb{Z}_3) = \mathbb{Z}_3.$$

$\square$

Hint: Prove using the universal property of tensors directly.

140 Quotients and Tensors – True or False? Let R be a ring, V a right R-

module, and W a left R-module. Then the additive group $V \otimes_R W$ is a quotient of the abelian group $V \otimes_{\mathbb{Z}} W$.

Proof: True. It is sufficient to construct a surjection from $V \otimes_{\mathbb{Z}} W$ to $V \otimes_R W$. To do this we follow the universal property: $f(v, w) = v \otimes_R w$. This is a well-defined map as it is the canonical middle linear map for $V \otimes_R W$; however, it may not be $\mathbb{Z}$-balanced. However recall that $\mathbb{Z}/m \leq R$ where $char\ R = m$ – possibly 0. So we can say for any $n \in \mathbb{Z}$ that $v \cdot n \in V$ as we take n to act on v as $n + m\mathbb{Z}$. Thus

$$f(vn, w) = vn \otimes w = v \otimes nw = f(v, nw).$$

It is clear that f is R-balanced so sums follow as required. Therefore f is $\mathbb{Z}$-balanced. Thus we have $f : V \otimes_{\mathbb{Z}} W \to V \otimes_R W$ which is clearly surjective as it is surjective on the pure tensors – the generators of these two abelian groups. □

141 Mixed Ring Tensors Give an example of a ring R, V a right R-module and W are left R-module such that $V \otimes_R W \not\cong V \otimes_Z W$ as abelian groups.

Hint: Consider $R = \mathbb{Z} \oplus \mathbb{Z}$.

Example: Let $R = \mathbb{Z} \oplus \mathbb{Z}$. Then

$$\mathbb{Z} \oplus_{\mathbb{Z}\oplus\mathbb{Z}} \mathbb{Z} \oplus \mathbb{Z} = \mathbb{Z}; \qquad \mathbb{Z} \oplus_{\mathbb{Z}} \mathbb{Z} \oplus \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}.$$

□

142 Fields and Tensors – True or False? If $K/\mathbb{Q}$ and $L/\mathbb{Q}$ are finite field extensions then $K \otimes_{\mathbb{Q}} L$ is a semi-simple artinian ring.

Hint: Use the dimension rule to conclude the extension is finite.

Proof: True.

As $dim_{\mathbb{Q}} K \otimes_{\mathbb{Q}} L = dim_{\mathbb{Q}} K dim_{\mathbb{Q}} L$ we see that as a vector space $K \otimes_{\mathbb{Q}} L$ is finite dimensional. Therefore it is trivially artinian as a $\mathbb{Q}$-algebra. Also we note that given $a \otimes b, c \otimes d \neq 0$ then $ac \otimes bd \neq 0$ as $ac \neq 0$ and $bd \neq 0$ and both K and L have no zero-divisors.

□

Chapter 4

Categories

5 If the functors $F : \mathscr{A} \to \mathscr{B}$ and $G : \mathscr{B} \to \mathscr{A}$ establish an equivalence of categories between $\mathscr{A}$ and $\mathscr{B}$ then F is both left and right adjoint to G.

Proof: Let

$$\begin{tikzcd}
FA \arrow[rrr, "Ff"] \arrow[ddd, "\alpha"] & & & FA' \arrow[ddd, "\alpha"] \\
 & A \arrow[ul] \arrow[r, "f"] \arrow[dl] & A' \arrow[ur] \arrow[dr] & \\
 & & & \\
GA \arrow[rrr, "Gf"'] & & & GA'.
\end{tikzcd}$$

$\square$

Chapter 5

Rings

---

1 Jacobson Radical – True or False? $J(\mathbb{R}[x]) = 0$.

Hint: Consider irreducible polynomials and there associated maximal ideals.

Proof: True. As we have a commutative ring, maximal left ideals are two-sided ideals. The maximal ideals of $\mathbb{R}[x]$ are those generated by irreducible polynomials (as $\mathbb{R}[x]$ is a PID).

Given the irreducible polynomials $x-n$ for $n \in \mathbb{Z}$ it follows each $I_n = (x-n)$ is a distinct maximal ideal of $\mathbb{R}[x]$. Also, $\cap_{n\in\mathbb{Z}} I_n = (p(x))$ since $\mathbb{R}[x]$ is a PID. Yet this requires $x - n|p(x)$ for all $n \in \mathbb{Z}$. Unfortunately no polynomial has infinitely many roots so no such $p(x)$ exists save $p(x) = 0$. Since $J(\mathbb{R}[x])$ is at least contained in this intersection we must conclude that $J(\mathbb{R}[x]) = \mathbf{0}$. $\square$

2 Jacobson Radical Let $R = \mathbb{R}[[x]]$. Calculate $J(R)$ and *Rad* R.

Hint: $\mathbb{R}[[x]]$ is an integral domain.

Example: Since $\mathbb{R}[[x]]$ is a local ring it follows $J(R) = (x)$. Moreover, $\mathbb{R}$ is an integral domain, so $\mathbb{R}[[x]]$ is an integral domain; thus, there are no zero-divisors, let alone nilpotent elements. Hence, *Rad* $R = \mathbf{0}$. $\square$

3 Primary Ideals The ideal $(4, 2x, x^2)$ in $\mathbb{Z}[x]$ is primary but not irreducible.

Hint: Show the quotient has no non-nilpotent zero-divisors.

Proof: Let $I = (4, 2x, x^2)$ and notice

$$(4) < (4, x^2) < (4, x^2, 2x).$$

Thus by the third isomorphism theorem we get:

$$R = \mathbb{Z}[x]/(4, x^2, 2x) \cong \frac{\mathbb{Z}[x]/(4)}{(4, x^2, 2x)/(4)} \cong \frac{\mathbb{Z}_4[x]/(x^2)}{(x^2, 2x)/(x^2)}.$$

Thus

$$R = \{0 + I, 1 + I, 2 + I, 3 + I, x + I, (x + 1) + I, (x + 2) + I, (x + 3) + I\}.$$

Now we simply check that all zero-divisors are nilpotent. First notice the elements $1 + I$, $3 + I$, $(x + 1) + I$, and $(x + 3) + I$ are all units, indeed of order 2, so they are not zero-divisors. Finally, $0 + I$, $2 + I$, $x + I$, and $(x + 2) + I$ are all nilpotent of order 2, so all zero-divisors are nilpotent. Hence I is primary in $\mathbb{Z}[x]$ – in particular it is $(2, x)$-primary, where $(2, x)$ is prime as its quotient is the field $\mathbb{Z}/2$.

However as suggested I is not irreducible as visibly

$$(4, 2x, x^2) = (4, x) \cap (2, x^2).$$

[$\mathbb{Z}[x]$ is a UFD so intersections are generated by all all minimal products, i.e.: $(4, 4x^2, 2x, x^2) = (4, 2x, x^2)$.] $\square$

4 Primary Containment The ideal $I = (x^2, 2x)$ in $\mathbb{Z}[x]$ is not primary, but $(x^2) < I < (x)$ and the ideal (x) is prime, and (x^2) is (x)-primary.

Hint: Show the quotient has a non-nilpotent zero-divisor.

Example: To show I is not primary it is sufficient to show that the quotient contains some non-nilpotent zero-divisor. To do this observe that

$$x(x + 2) = x^2 + 2x \equiv 0 \pmod{I}$$

yet

$$(x+2)^m = (x+2)^2(x+2)^{m-2} = (x^2+4x+4)(x+2)^{m-2} \equiv 4(x+2)^{m-2} \pmod{I}$$

So if $(x+2)$ is nilpotent mod I, then 4 is a zero-divisor mod I and so would also be nilpotent. However $4^i \notin I$ as x has no inverse in I, and so 4 is not nilpotent so either it is not a zero-divisor in which case $(x+2)$ is a criminal element, or it is itself a non-nilpotent zero-divisor. In either event, I is not primary.

That (x) is primary follows from that fact that $\mathbb{Z}[x]/(x) = \mathbb{Z}$ which is an integral domain. That (x^2) is (x)-primary follows from the fact that for all $ab \in (x^2)$ where $a \notin (x^2)$ we see $x^2|ab$ so $x^2 \nmid a$ so $x|b$ for certain $b \in (x)$ and $\sqrt{(x^2)} = (x)$. □

Hint: Recall that $\mathbb{Z}[x]$ is a UFD so irreducible factors are immutable.

5 Primary Decomposition Represent the ideal $(9, 3x+3)$ in $\mathbb{Z}[x]$ as the intersection of primary ideals.

Example: Since $\mathbb{Z}$ is a UFD so is $\mathbb{Z}[x]$. Thus intersections can be detected by divisors. Consider the intersection $(3) \cap (9, x+1)$. Any element in the intersection must be divisible by 3, and furthermore also by either 9 or by $x+1$. In the first case then the element is simply divided by 9, so indeed we must include the minimal version of such an element – 9 itself. In the later case as $3(x+1)$ divides the element, then $3x+3$ must be in the intersection as well. Given any element in the intersection it is characterized by being divided by either 9 or $3x+3$ thus the intersection is precisely $(9, 3x+3)$. □

Hint: Pass to R/I and notice $\sqrt{I}/I$ is now the nil-radical of R/I.

6 Maximal Radicals Let I be an ideal of a commutative ring R such that $\sqrt{I}$ is a maximal ideal in R. Prove that I is primary.

Proof: Given that $\sqrt{I}$ is a maximal ideal we see that in R/I, $\sqrt{I}/I$ is also a maximal ideal. Given any $x+I$ which is nilpotent, it follows $x^n + I = I$ so $x^n \in I$ and we now see that $\sqrt{I}/I$ is precisely the nil-radical of R/I. So it is the intersection of all prime ideals in R/I. Yet this implies, by the maximality of $\sqrt{I}/I$, that $\sqrt{I}/I$ is the only prime ideal in R/I, so also the only maximal ideal in R/I. Hence R/I is a local ring and indeed $\sqrt{I}/I$ must contain all non-units. In particular, all zero-divisors. However, moments ago we notice, $\sqrt{I}/I$ is the nil-radical so it contains nothing but the nilpotent elements of the ring R/I so is follows all zero-divisors of R/I are nilpotent, and so this characterizes I as a primary ideal in R. □

Hint: Notice $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

7 Associated Primes In a noetherian ring, prove that $\sqrt{I}$ is the intersection of the associated prime ideals of I.

Proof: Let

$$I = Q_1 \cap \cdots \cap Q_n$$

be an irredundant primary decomposition of I, with $P_i = \sqrt{Q_i}$ the associated primes. These associated primes are uniquely determined in a noetherian ring by the Lasker-Noether theorem.

It follows $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ as given any $x^n \in I \cap J$ clearly $x^n \in I$ and J so $x \in \sqrt{I} \cap \sqrt{J}$, and the process is reversible.

Finally

$$\sqrt{I} = \sqrt{Q_1 \cap \cdots \cap Q_n} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_n}.$$

□

Hint: Inverting the invertible elements should not change anything.

8 Localization Let $S = \mathbb{Z}_m^\times$ be the set of all units in $\mathbb{Z}_m$ (equivalently the set of all non-zero-divisors,) and determine $S^{-1}\mathbb{Z}_m$.

Example: Consider the equivalence relation: $\frac{a}{b} = \frac{c}{d}$ if and only if for some $u \in S$ we have $u(ad - bc) = 0$. However, u is in S so by the choice of S, u is not a zero-divisor, and hence we must have $ad = bc$. Hence

$$\left[\frac{r}{s}\right] = \left\{\frac{rt}{st} \;:\; t \in S\right\}.$$

In particular, as all elements of S are units, each r/s can be expressed as $r'/1$. Thus we see a canonical isomorphism between $\mathbb{Z}_m$ and $S^{-1}\mathbb{Z}_m$. $\square$

9 Localization Let S be a multiplicative subset of R and T be a multiplicative subset of $S^{-1}R$. Let $S_* = \{r \in R : \left[\frac{r}{s}\right] \in T \text{ for some } s \in S\}$. Then S_* is a multiplicative subset of R and there is a ring homomorphism $S_*^{-1}R \cong T^{-1}(S^{-1}R)$.

Hint: Use the universal property of localization.

Proof: Given any $a, b \in S_*$ it follows there exist $s, t \in S$ for which $\frac{a}{s}, \frac{b}{t} \in T$. This means $st \in S$ as S is multiplicative and furthermore, $\frac{ab}{st} \in T$ as T is multiplicative. Therefore $ab \in S_*$. Given that $1 \in T$, then for any $s \in S$, $\frac{s}{s} \in T$ proving $S \subseteq S_*$ and so specifically $1 \in S_*$ proving S_* is multiplicative itself.

Now define the map:

$$f : R \to T^{-1}(S^{-1}R) : r \mapsto \frac{r/1}{1/1}$$

and we quickly verify this is an R-homomorphism. Through the universal property we now get an $S_*^{-1}R$-homomorphism

$$\hat{f} : S_*^{-1}R \to T^{-1}(S^{-1}R) : \frac{r}{s} \mapsto \frac{r/s}{s/s'},$$

where $s' \in S$ is any such that $s/s' \in T$. By the universal property applied T we get another map

$$\hat{g} : T^{-1}(S^{-1}R) \to S_*^{-1}R : \frac{r/s}{t/s'} \mapsto \frac{rs'}{st}.$$

It follows routinely that $fg = id$ and $gf = id$ so this is an isomorphism. $\square$

10 Localized Local Rings – True or False? If R is a local ring, then there is a commutative ring R' and a prime ideal P of R' such that $R \cong R'_P$.

Hint: Localize on the unique maximal ideal.

Proof: Let P be the unique maximal ideal in R. As such, P contains all non-units of R. Indeed, P is also prime as it is maximal. Thus letting $R' = R$ we see that $R'_P \cong R$. $\square$

11 Localization of Primes Let $\mathfrak{p}$ be a prime ideal of R. Show that $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ is isomorphic to the field of quotients of $R/\mathfrak{p}$.

Hint: Use the universal property of localization.

Proof: Define a map $f : R \to Fr(R/\mathfrak{p})$ as $f(r) = [r + \mathfrak{p}/1 + \mathfrak{p}]$. This definition makes sense as it is simply the composition of the canonical projection map $R \to R/\mathfrak{p}$ followed by the canonical inclusion map $R/\mathfrak{p} \to Fr(R/\mathfrak{p})$, and thus there is no need to verify f is an R-algebra homomorphism. More importantly, we see given any $s \notin \mathfrak{p}$, $f(s) \neq 0$ so $f(s)$ is invertible. Thus we have from the universal property of localization the following:

$$\begin{tikzcd} R \arrow[r, "\mu"] \arrow[dr, "f"'] & R_\mathfrak{p} \arrow[d, "\hat{f}"] \\ & Fr(R/\mathfrak{p}). \end{tikzcd}$$

Given any $[r + \mathfrak{p}/s + \mathfrak{p}] \in Fr(R/\mathfrak{p})$

$$\left[\frac{r+\mathfrak{p}}{s+\mathfrak{p}}\right] = \left[\frac{r+\mathfrak{p}}{1+\mathfrak{p}}\right]\left[\frac{s+\mathfrak{p}}{1+\mathfrak{p}}\right]^{-1} = f(r)f(s)^{-1} = \hat{f}([r]_\mathfrak{p})\hat{f}([s]_\mathfrak{p})^{-1} = \hat{f}\left(\left[\frac{r}{s}\right]_\mathfrak{p}\right).$$

Hence $\hat{f}$ is surjective. Now we inspect the kernel.

Given $[r/s]_{\mathfrak{p}}$ in the kernel of $\hat{f}$ it follows $[f(r)/f(s)] = [0/1]$ in $Fr(R/\mathfrak{p})$. Hence $f(r) = 0$ and so $r \in Ker\ f$. This implies $r \in \mathfrak{p}$ since the kernel of f is determined entirely by the projection of $R \to R/\mathfrak{p}$. Hence $[r/1]_{\mathfrak{p}} \in \mathfrak{p}_{\mathfrak{p}}$ and since $\mathfrak{p}_{\mathfrak{p}}$ is and ideal it follows that in fact $[r/s]_{\mathfrak{p}}$ is contained in $\mathfrak{p}_{\mathfrak{p}}$. Therefore the kernel of $\hat{f}$ is contained in $\mathfrak{p}_{\mathfrak{p}}$. It is not difficult to see the reverse of this inclusion as well. So we conclude that the kernel of our map is precisely $\mathfrak{p}_{\mathfrak{p}}$ and so by the first isomorphism theorem we have

$$R_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} \cong Fr(R/\mathfrak{p}).$$

□

Hint: Show $(x, 2)$ is a maximal ideal and invoke Exercise-5.6.

12 Primary Ideals – True or False? The ideal $(x^2, 4)$ is $(x, 2)$-primary in $\mathbb{Z}[x]$.

Proof: True. Clearly $\sqrt{(x^2, 4)}$ contains $(x, 2)$, and since the quotient $\mathbb{Z}[x]/(x, 2) = \mathbb{Z}/2$ it is clear that $(x, 2)$ is prime and indeed maximal so it must be the radical. Now we appeal to the fact of Exercise-5.6 that all ideals whose radicals are maximal are primary to this radical. □

Hint: Use Nakayama's Lemma.

13 Local Rings Let R be a noetherian local ring with maximal ideal M and let $x_1, \dots, x_n \in M$. Suppose that $\{x_1 + M^2, \dots, x_n + M^2\}$ is a basis of the R/M-vector space M/M^2. Show that $M = Rx_1 + \cdots + Rx_n$.

Proof: First notice since M is and ideal of R that M^2 is also an ideal. Thus we have M/M^2 as an ideal of R/M^2 and so M/M^2 is an R/M^2-module. Thus we are free to take the quotient module $(M/M^2)/(M \cdot M/M^2) = M/M^2$ as and R/M-module. So the question makes sense.

Take $N = Rx_1 + \cdots + Rx_n$ which is clearly contained in M. As this is a basis for M/M^2 as an R/M-module, it follows $M = N + M^2 = N + MM$. However R is a local ring so $J(R) = M$. This means we have the setup of Nakayama's lemma: $M = N + J(R)M$ and so $M = N$. We see $M = R$. □

Hint: P must be the nil-radical.

14 Nil-Radical Let R be a commutative ring with a unique prime ideal P and let $r \in R$. Prove that x is nilpotent if and only if $x \in P$.

Proof: Since R has only one prime ideal then $Rad\ R = P$ so P contains all nilpotent elements and indeed is all nilpotent elements. □

Hint: Consider (x, y).

15 Polynomial Rings – True or False? $\mathbb{C}[x, y]$ is a PID.

Example: False. Consider the ideal (x, y). Since $\mathbb{C}[x, y]/(x, y) \cong \mathbb{C}$ it follows (x, y) is a proper maximal ideal and thus prime. Now we must make sure it is not principal.

Suppose $(p(x, y)) = (x, y)$. Then $x|p(x, y)$ and $y|p(x)$ so indeed $xy|p(x, y)$. However it follows then that $x = q(x)p(x, x)$ for some $q(x)$ in $\mathbb{C}[x]$. Yet as $xy|p(x, y)$ it follows $x^2|p(x, x)$ so by a degree argument we see we reach a contradiction. Hence (x, y) is not principal. □

Hint: Use the Hilbert Basis Theorem.

16 Noetherian Rings – True or False? $\mathbb{C}[x, y]$ is a noetherian ring.

Proof: True. By the Hilbert basis theorem any polynomial ring over a noetherian ring is noetherian. Hence $\mathbb{C}[x]$ is noetherian and so also $\mathbb{C}[x][y] = \mathbb{C}[x, y]$. □

$\mathbb{Q}$.

17 Artinian Rings – True or False? Every subring of an artinian ring is artinian.

Example: False. Since $\mathbb{Q}$ is a field it is artinian. However it clearly contains the non-artinian ring $\mathbb{Z}$ which has an infinite descending chain

$$(2) > (4) > (8) > \cdots .$$

$\square$

18 UFDs – True or False? $\mathbb{Z}[x]$ is a UFD.

Hint: Polynomials over UFDs are UFDs.

Proof: True. Since $\mathbb{Z}$ is a PID it is also a UFD, and as polynomial rings over a UFD are a UFD we see indeed $\mathbb{Z}[x]$ is a UFD. $\square$

19 Noetherian Rings – True or False? $\mathbb{Z}[x,y]/(x-2y)$ is a noetherian ring.

Hint: Quotients of noetherian Rings are noetherian.

Proof: True. As $\mathbb{Z}$ is noetherian, the Hilbert basis theorem tells us so is $\mathbb{Z}[x,y]$. We also no quotients of noetherian rings are noetherian by the correspondence theorem. So $\mathbb{Z}[x,y]/(x-2y)$ is noetherian. $\square$

20 Noetherian PIDs – True or False? If R is a PID then R is noetherian.

Hint: Every non-zero non-unit in R has a finite unique factorization into primes.

Proof: Given any chain of principal ideals

$$\mathbf{0} < (r_1) \leq (r_2) \leq \cdots .$$

It follows $r_i | r_{i-1} | \cdots | r_2 | r_1$. However in a PID we may factor $r_1 \neq 0$ into a finite unique set of irreducibles with difference only by a unit. So unless $r_i = r_j$ for all $i < j$ for sufficiently large i, we will run out of irreducibles to eliminate from r_1. Thus the chain stabilizes in finitely many steps. $\square$

21 Prime Ideals – True or False? If R is a noetherian ring then every non-zero prime ideal of R is maximal.

Hint: Consider $\mathbb{C}[x,y]$.

Example: False. Consider $\mathbb{C}[x,y]$. By the Hilbert basis theorem this is a noetherian ring. Furthermore, $(x) < (x,y)$ and both are prime since their quotients give the integral domains $\mathbb{C}[y]$ and $\mathbb{C}$ respectively. However visibly (x) is not maximal. $\square$

22 Prime Ideals – True or False? If R is a UFD then every non-zero prime ideal of R is maximal.

Hint: Consider $\mathbb{C}[x,y]$.

Example: False. Consider $k[x,y]$, with k any field. Since k is a field it is a PID and so also a UFD. Hence $k[x]$ is a UFD so indeed $k[x][y] = k[x,y]$ is a UFD. Notice $k[x,y]/(y) \cong k[x]$ which is an integral domain so (y) is a prime ideal. Yet $k[x]$ is not a field as x has no inverse. $\square$

23 UFDs – True or False?

Hint: Use the subring $\mathbb{Z}[\sqrt{10}]$ of $\mathbb{R}$.

(a) Every quotient ring of a UFD is a UFD.

(b) Every subring of a UFD is a UFD.

Example:

(a) False. Consider $\mathbb{Z}$ which is a PID and so also a UFD. The quotient $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain so in particular it is not a UFD.

(b) False. Consider the ring $R = \{a + b\sqrt{10} \ : \ a, b \in \mathbb{Z}\}$ as a subring of $\mathbb{R}$. Certainly the field $\mathbb{R}$ is a UFD, but we need to verify R is not. Notice

$$2 \cdot 3 = 6 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

Now we must verify that all these are irreducible. We do this in parts with some tools.

(i) There exists a norm function $N : R \to \mathbb{Z}$ such that $N(xy) = N(x)N(y)$, and $N(x) = 0$ if and only if $x = 0$.

(ii) $N(u) = \pm 1$ if and only if u is a unit in R.

(i) Define the norm of an element $x = a + b\sqrt{10}$ to be $x\overline{x}$ where $\overline{x} = a - b\sqrt{10}$, so that $N(x) = a^2 - 10b^2 \in \mathbb{Z}$. Let $x = a + b\sqrt{10}$ and $y = c + d\sqrt{10}$ be arbitrary elements of R.

$$\begin{aligned} N(xy) &= N((ac + 10bd) + (ad + bc)\sqrt{10}) = (ac + 10bd)^2 - 10(ad + bc)^2 \\ &= a^2c^2 + 100b^2d^2 - 10a^2d^2 - 10b^2c^2 = (a^2 - 10b^2)(c^2 - 10d^2) \\ &= N(x)N(y). \end{aligned}$$

When $x = 0$ it is clear $N(x) = 0$. Given $N(x) = 0$ it follows $a^2 - 10b^2 = 0$; therefore, $a^2 = 10b^2$ and so $|a| = |b|\sqrt{10}$. So either a is not an integer or b is not, unless both are zero; so $x = 0$. Hence, $N(x) = 0$ if and only if $x = 0$.

(ii) Suppose $uv = 1$ for two elements u, v in R. Applying the norm function it is clear $N(u)N(v) = N(uv) = N(1) = 1$. Since N maps only into the integers and only 1 and -1 have multiplicative inverses in $\mathbb{Z}$ it follows $N(u) = \pm 1$.

Now we may prove that the elements are irreducible. Suppose $2 = uv$ for two non-units u and v in R. Then $N(u)N(v) = N(2) = 4$ and with u and v being non-units it is forced that $N(u) = \pm 2$. Let $u = a + b\sqrt{10}$ and consider the equation $a^2 - 10b^2 = N(u) = \pm 2$. Since the equation is true in the integers it must be true in its factor rings; therefore, $a^2 - 10b^2 \equiv 2 \pmod 5$. However no element exists in $\mathbb{Z}/5\mathbb{Z}$ such that $a^2 = 2$ (proved by testing all five elements.) So no u exists in R with the property $N(u) = \pm 2$ concluding by contradiction that 2 is irreducible in R.

Again suppose $3 = uv$ with u and v again non-unit elements. Picking up the pace suppose $a^2 - 10b^2 = N(u) = \pm 3$. Then $a^2 - 10b^2 \equiv 3 \pmod 5$ but once again $a^2 \neq 3 \bmod 5$ for any elements a. Therefore 3 is irreducible in R.

Finally $N(4 \pm \sqrt{10}) = 16 - 10 = 6$. Suppose $4 \pm \sqrt{10} = uv$ for non-units u and v. Then clearly $N(u)N(v) = 6$ and thus $N(u) = \pm 2$ or ± 3 however from the above argument it is clear no such element exists therefore $4 \pm \sqrt{10}$ is irreducible.

□

Hint: Consider $\mathbb{Z}$.

24 Prime Intersection – True or False? The intersection of prime ideals in a commutative ring is prime.

Example: False. Consider $\mathbb{Z}$ where primes correspond precisely to maximal ideals $p\mathbb{Z}$ where p is a prime number. Here

$$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$$

which is not prime. □

25 Tensors – True or False? If R is a local ring with maximal ideal M and V is a finitely generated R-module with $(R/M)\otimes_R V = \mathbf{0}$ then $V = \mathbf{0}$.

Hint: Consider $V \leq M$.

Example: False. Let $R = \mathbb{C}[[x]]$ and take $M = V = (x)$. Certainly V is a finitely generated R module, and R is also a local ring. Furthermore, $R/M \otimes_R V \cong \mathbf{0}$ since

$$a(x) + M \otimes b(x)x = a(x)x + M \otimes b(x) = M \otimes_R b(x) = 0 + M \otimes b(x) = 0.$$

However $V \neq \mathbf{0}$. □

26 Prime Ideals – True or False? If R is an integral domain and $r \in R$ is an irreducible element of R, then (r) is a prime ideal of R.

Hint: Work in ring which is not a UFD.

Example: False. Refer back to the example in Exercise-23. Here R was taken to be $\mathbb{Z}[\sqrt{10}]$. Recall

$$2 \cdot 3 = 6 = (4+\sqrt{10})(4-\sqrt{10}).$$

Suppose 2 is prime. Then $R/(2) = \mathbb{Z} + \mathbb{Z}\sqrt{10}$ has a nilpotent element $\sqrt{10}$ as

$$(\sqrt{10})^2 = 10 \equiv 0 \pmod 2.$$

Therefore we do not have an integral domain in the quotient so 2 is not prime. □

27 Primary Ideals Show that if Q is a primary ideal in a commutative ring R, then $\sqrt{Q}$ is a prime ideal. Show the converse holds if R is a PID.

Hint: Use the prime element and division properties for the converse.

Proof: Consider $ab \in \sqrt{Q}$. We wish to show $a \in \sqrt{Q}$ or $b \in \sqrt{Q}$. Without loss of generality let $a \notin \sqrt{Q}$. Thus $a^n \notin Q$ for any $n > 0$. However as $ab \in \sqrt{Q}$ it follows $a^n b^n = (ab)^n \in Q$ for large enough n. Now using the definition of primary we see that $a^n \notin Q$ implies $b^n \in \sqrt{Q}$. But then $b^{nm} \in Q$ for some $m > 0$, so indeed $b \in \sqrt{Q}$ – using the elemental definition of the radical ideal. Therefore $\sqrt{Q}$ is prime.

Now assume R is a PID and that $\sqrt{Q}$ is prime for some ideal Q. We will show Q is $\sqrt{Q}$-primary. As R is a PID there exists an element – a prime element – p such that $\sqrt{Q} = (p)$. Also take $Q = (q)$. Then $p\sqrt{Q}$ by definition implies $q|p^n$. But $(q) \leq (p)$ implies $p|q$ so $q = p^i$ for some $i \geq 0$. Therefore $Q = \sqrt{Q}^i$. But any prime to a power is primary. □

28 Units Let R be an integral domain and F its field of fractions. Then $r \in R$ is a unit if and only if $\frac{1}{r} \in F$ is integral over R.

Hint:

Proof: Let $r \in R$ be a unit. It follows $\frac{1}{r} \in R$ and so $x - \frac{1}{r} \in R[x]$ so indeed $\frac{1}{r}$ is integral over R.

Now suppose $\frac{1}{r} \in F$ is integral over R. Then there exists a monic polynomial $p(x) = x^n + \cdots + a_0 \in R[x]$ such that $p(1/r) = 0$. That is:

$$\begin{aligned}
\frac{1}{r^n} + \cdots + \frac{a_1}{r} + a_0 &= 0; \\
\frac{1}{r} + \cdots + a_1 r^{n-2} + a_0 r^{n-1} &= 0 \\
\frac{1}{r} &= -a_{n-1} - a_{n-2}r - \cdots - a_0 r^{n-1} \in R.
\end{aligned}$$

□

29 Localization of Ideals – True or False? Let S be a proper multiplicative subset of a commutative ring R and $I \neq J$ be ideals of R. Then $S^{-1}I \neq S^{-1}J$.

Hint: Conside an ideal which tain I or J.

Example: False. Let $R = \mathbb{Z}$ and $I = 3\mathbb{Z}$ and $J = 5\mathbb{Z}$. Clearly $I \neq J$. Now consider $\mathfrak{p} = 2\mathbb{Z}$ and localize over $\mathfrak{p}$. Thus $I_{\mathfrak{p}} = R_{\mathfrak{p}} = J_{\mathfrak{p}}$ as we now have both 3 and 5 as units. □

Hint: Expand and contract the intersection of prime ideals over I.

30 Localization and Radicals – True or False? Let S be a proper multiplicative subset of a commutative ring R and I be an ideal of R. Then $\sqrt{S^{-1}I} = S^{-1}\sqrt{I}$.

Proof: True. Let $\sqrt{I} = \bigcap_{I \leq P} P$ where P is a prime in R. If P is prime in R then $S^{-1}P = R$ or $S^{-1}P$ is prime in $S^{-1}R$. In particular when P avoids S we know $S^{-1}P^C = P$. So we see for every prime Q of $S^{-1}R$ there exists a prime $P \in R$ such that $Q = S^{-1}P$. Moreover as the extension is order preserving, $I \leq P$ if and only if $S^{-1}I \leq S^{-1}P$. Thus we have

$$S^{-1}\sqrt{I} = S^{-1}\bigcap_{I \leq P} P = \bigcap_{I \leq P} S^{-1}P = \bigcap_{S^{-1}I \leq S^{-1}P} S^{-1}P = \sqrt{S^{-1}I}.$$

□

Hint: Notice the complement of S is the prime ideal of all graphs that pass through the origin.

31 Localization The ring $R = \mathbb{R}[x, y]$ is localized at the multiplicative set $S = \{f(x, y) \in R \mid f(0, 0) \neq 0\}$. Find all maximal ideals of $S^{-1}R$ and its Jacobson radical.

Example: Localized rings are local so we are searching for a unique maximal ideal. The complement of S is the set P of all polynomials $g(x, y) \in \mathbb{R}[x, y]$ whose graph passes through the origin. Given any two polynomials $g(x, y), h(x, y) \in \mathbb{R}[x, y]$ for which $g(x, y)h(x, y) \in P$ it follows $g(0, 0)h(0, 0) = 0$ so either g or h is in P. Clearly P is closed to sums and products and absorbs products so P is a prime ideal. Therefore we are localizing at P. So the maximal ideal is $P_P = P$, and the Jacobson radical is P_P as well [in commutative rings the Jacobson radical is the intersection of maximal ideals.] □

Hint: Show that any element outside R in the intersection is equal to a fraction of elements that must be in R.

32 Localization of Domains Let R be an integral domain with a quotient field F. Prove that for any maximal ideal M of R, R_M can be canonically embedded into F and $\bigcap_M R_M = R$.

Proof: The embedding follows form the universal property. Take any proper multiplicative set S in R. Starting with the inclusion map of R into F we notice $\iota(r)$ is invertible in F so long as $r \neq 0$. Hence all elements $s \in S$ have the property $\iota(s)$ is invertible in F. So by the universal property of either F or $S^{-1}R$ we see ι extends to a ring homomorphism $\hat{\iota} : S^{-1}R \to F$. Furthermore, if $\hat{\iota}(r/s) = 0$ then $\iota(r) = 0$ so $r = 0$ proving we have a canonical embedding.

Now consider the intersection $R' = \bigcap_M R_M$ where M is a maximal ideal of R. As $R \leq R_M$ for each M we see $R \leq R'$. Take any $x \in R'$. If $x \notin R$ then define $I = \{y \in R \mid yx \in R\}$. As $0 \in I$, I is non-empty. Also $r \in R$, $y \in I$ gives us $ryx \in R$ so $ry \in I$. The closure of sums is also clear so I is an ideal of R and so it is contained in some maximal ideal M as clearly $1 \notin I$. Notice that $x \in R_M$ as it is in the intersection of all such localizations. This means there exist a $w \notin M$ and $r \in R$ such that $x = r/w$. Yet this implies $wx = r \in R$ and so $w \in I$ which it cannot be as $I \leq M$. The contradiction implies $x \in R$ in the first place. □

33 Localized Modules Let R be a commutative ring and V be an R-module. Show that $V = \mathbf{0}$ if and only if $V_M = \mathbf{0}$ for every maximal ideal M of R.

Hint: Use the maximal ideal containing the annihilator of V.

Proof: Suppose that $V = \mathbf{0}$ then clearly $V_M = \mathbf{0}$.

Now suppose that $V_M = \mathbf{0}$ for every localization R_M at a maximal ideal M. If $V = \mathbf{0}$ we are done. So assume it is non-trivial so that we know its annihilator is a proper ideal of R. Thus there exists a maximal ideal M in R containing the annihilator of V. We localize R at M and consider V_M we notice that $V \leq V_M$ as $v/1 \neq 0$ unless $v = 0$. Yet $V_M = \mathbf{0}$ so $V = \mathbf{0}$. $\square$

34 Integral Fields Let A be a domain which is integral over R. Prove that A is a field if and only if R is as well.

Hint: Recall the result of Exercise-5.28: integral units are contained in the ring.

Proof: Suppose A is a field. Using Exercise-5.28 we know if any element of R is a unit in A then it is also a unit R, so therefore all non-zero elements in R are invertible because they are in A.

Now suppose R is a field. Then we use Lemma-5.3.21 to conclude A is a field. $\square$

35 Integral Closure – True or False? The ring $\mathbb{Q}[x, y]$ is integrally closed.

Hint: Show it is a UFD.

Proof: True. Notice that $\mathbb{Q}$ is a PID so it is a UFD and as polynomial rings over UFDs are UFDs we may conclude $\mathbb{Q}[x, y]$ is a UFD. Now we conclude by recalling all UFDs are integrally closed. $\square$

36 Integral Closure – True or False? The ring $\mathbb{Q}(x)[y]$ is integrally closed.

Hint: Show it is a UFD.

Proof: True. Notice $\mathbb{Q}(x)$ is a field so it is PID and thus a UFD − although trivially so. Hence $\mathbb{Q}(x)[y]$ is a UFD so as all UFDs are integrally closed we conclude that $\mathbb{Q}(x)[y]$ is integrally closed. $\square$

37 Integral Closure – True or False? The ring $\mathbb{Z}[x]$ is integrally closed.

Hint: Show it is a UFD.

Proof: True. Notice that $\mathbb{Z}$ is a PID so it is a UFD and as polynomial rings over UFDs are UFDs we may conclude $\mathbb{Z}[x]$ is a UFD. Now we conclude by recalling all UFDs are integrally closed. $\square$

38 Integral Closure Let R be a commutative integral domain. Prove that if $R_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$ of R, then R is integrally closed.

Hint: Recall that R is the intersection of the localization at maximal ideals – Exercise-5.32.

Proof: Let $a \in \overline{R}$. As such there exists a monic polynomial $f(x) \in R[x]$ for which $f(a) = 0$. Now recall that R is a domain so in $R_{\mathfrak{p}}$ we have R canonically embedded as $\frac{r}{1} = \frac{r'}{1}$ if and only if $ur = ur'$ for some $u \notin \mathfrak{p}$. But being a domain this is equivalent to $r = r'$. As such, $f(x) \in R[x] \subseteq R_{\mathfrak{p}}[x]$ so we see indeed $a \in \overline{R}_{\mathfrak{p}}$ for all $\mathfrak{p}$ so it is in the intersection of all these.

Now that we see the integral closure of the the local rings contains the integral closure of R we may use our assumption that $\overline{R}_{\mathfrak{p}} = R_{\mathfrak{p}}$ to continue. Recall that R is embedded in each $R_{\mathfrak{p}}$ and that every maximal ideal M is prime; thus

$$R \subseteq \bigcap_{\mathfrak{p}} R_{\mathfrak{p}} \subseteq \bigcap_{M} R_M = R.$$

Hence

$$a \in \bigcap_{\mathfrak{p}} R_{\mathfrak{p}} = R,$$

illustrating $\overline{R} \subseteq R$ so naturally $\overline{R} = R$. $\square$

Hint: Use Krull's intersection theorem.

39 Idempotent Ideals Let R be a commutative noetherian local ring with maximal ideal M which satisfies $M^2 = M$. Prove that R is a field.

Proof: From Krull's intersection theorem we know $J = \bigcap_{n>0} M^n = M$ and as R is local $J = \mathbf{0}$; hence, $M = \mathbf{0}$ and this was a maximal ideal so indeed R is a field as $R/M \cong R$ and R/M is a field. $\square$

Hint: Consider $\mathbb{Z}/4$.

40 Finite Local Rings – True or False? Every finite local ring is a field.

Example: False, and we may as well use the smallest example $\mathbb{Z}/4$. The subring $\{0, 2\}$ is an ideal as discovered empirically $[1\{0, 2\} = \{0, 2\}, 3\{0, 2\} = \{0, 2\}.]$ Moreover the other non-zero elements are units so they cannot be adjoined to a proper ideal; hence, $\mathbb{Z}/4$ is a local ring. However $2 \cdot 2 \equiv 0 \pmod 4$ so it is not a field. $\square$

Hint: The only prime ideal in such a ring is the unique maximal ideal.

41 Local Artinian Rings – True or False? A local artinian ring has finitely many prime ideals.

Example: True. In fact we will prove that the only prime ideal in such a ring is the lone maximal ideal. Begin by letting J be the maximal ideal which we notice is also the Jacobson radical as the ring is local. Now any prime ideal P must be contained in J by the maximality. However, notice that our ring is artinian so there exists some n such that $J^n = \mathbf{0}$ – the Jacobson radical is nilpotent. As such, suppose, $J \neq P$ so that we may take an element $x \in J - P$. This element is non-trivial in the quotient R/P. Moreover, $x^n = 0$ as $x \in J$, so $(x + P) = x^n + P = 0 + P = P$ so there is a nilpotent element in the quotient. Therefore P is not prime. Hence the only prime ideal in a local artinian ring is the maximal ideal itself. $\square$

Hint: It is primary.

42 Primary Decomposition Let $R = \mathbb{R}[x, y]$, and

$$I = \left\{ f(x, y) \in R : f(0, 0) = \frac{\partial f}{\partial x}(0, 0) = \frac{\partial f}{\partial y}(0, 0) \right\}.$$

Check that I is an ideal of R and determine if it is maximal, prime, primary, or determine is primary decomposition.

Example: Let $f \in I$ and $g \in R$. Consider the product gf (R is commutative so this is sufficient)

$$\begin{aligned}
gf(0,0) &= g(0,0)f(0,0) = g(0,0)0 = 0; \\
\frac{\partial}{\partial x} fg(0,0) &= g(0,0)\frac{\partial f}{\partial x}(0,0) + \frac{\partial g}{\partial x}(0,0)f(0,0) = 0; \\
\frac{\partial}{\partial y} fg(0,0) &= g(0,0)\frac{\partial f}{\partial y}(0,0) + \frac{\partial g}{\partial y}(0,0)f(0,0) = 0.
\end{aligned}$$

Hence I absorbs product. Notice $f(x, y) = 0$ is an element in I so I is non-empty. Also given $f, g \in I$ we have

$$\begin{aligned}
(f+g)(0,0) &= f(0,0) + g(0,0) = 0; \\
\frac{\partial}{\partial x}(f+g)(0,0) &= \frac{\partial f}{\partial x}(0,0) + \frac{\partial g}{\partial x}(0,0) = 0; \\
\frac{\partial}{\partial y}(f+g)(0,0) &= \frac{\partial f}{\partial y}(0,0) + \frac{\partial g}{\partial y}(0,0) = 0.
\end{aligned}$$

Thus $f + g \in I$. Therefore I is an ideal of R.

Notice $x^2 \in I$ but $x \notin I$ proving that I is not prime, and so also not maximal. In particular notice

$$I = (x^i y^j \; : \; i + j \geq 2, i, j \geq 0).$$

Hence

$$\sqrt{I} = (x, y)$$

as x^2 and y^2 are in I and the $x^i y^j$ terms are all contained in (x, y). Notice $\sqrt{I}$ is therefore prime so I is $\sqrt{I}$-primary and so we have its primary decomposition. □

43 Algebraic Extensions Let M be a maximal ideal of $\mathbb{Q}[x, y, z]$. Prove that $F = \mathbb{Q}[x, y, z]/M$ is a finite algebraic extension of $\mathbb{Q}$.

Hint: Only the finiteness is in question.

Proof: It is clear that a quotient of $R = \mathbb{Q}[x, y, z]$ does not introduce any transcendental elements, so indeed F is an algebraic extension of $\mathbb{Q}$. What must be determined is why the degree of the extension is finite.

Consider localizing R at M. It still follows that $R_M/M_M \cong F$. However now we recall that R is a noetherian ring so M is generated by finitely many irreducibles. **PENDING:** figure out. □

44 Integrality of Polynomials Let R be a domain. Then R is integrally closed if and only if $R[x]$ is integrally closed.

Hint:

Proof: Suppose $\overline{R} = R$. It is clear that $R[x]$ is a domain since R is and as such $R[x]$ is integrally closed if it is so inside $Fr(R[x]) = Fr(R)(x)$. Suppose we take a reduced fraction $f(x)/g(x) \in \overline{R[x]}$. This means there exists a monic polynomial $h(x, y) \in R[x][y]$ for which $h(x, f(x)/g(x)) = 0$. Since h is monic it follows the leading coefficient is 1 and supposing the degree is n we see:

$$\begin{aligned}
h(x, f(x)/g(x)) &= \frac{f(x)^n}{g(x)^n} + \sum_{i=0}^{n-1} r_i(x) \frac{f(x)^i}{g(x)^i} = 0; \\
\frac{f(x)^n}{g(x)^n} &= -\sum_{i=0}^{n-1} r_i(x) \frac{f(x)^i}{g(x)^i}; \\
f(x)^n &= -\sum_{i=0}^{n-1} r_i(x) f(x)^i g(x)^{n-i} = g(x) \left(-\sum_{i=0}^{n-1} r_i(x) f(x)^i g(x)^{n-i-1} \right).
\end{aligned}$$

Hence $g(x) | f(x)$ and as this is reduced we have $g(x) = 1$. As such $f(x) \in Fr(R)[x]$. We must show that indeed $f(x) \in R[x]$. **PENDING:** slay this dragon! It is sufficient to show $\overline{R[x]} \leq \overline{R}[x]$. How is not yet known.

For the reverse direction we play set theory: Let $R[x] = \overline{R[x]}$; thus $R \subseteq \overline{R} \subseteq \overline{R[x]} = R[x]$ so

$$R = R \cap Fr(R) \subseteq \overline{R} \cap Fr(R) = \overline{R} \subseteq \overline{R[x]} \cap Fr(R) = R[x] \cap Fr(R) = R.$$

Hence $\overline{R} = R$. □

45 Integral Closures and Polynomials Let $R \subseteq A$ be rings with R integrally closed in A. Suppose that $h(x)$ is a polynomial in $R[x]$ which factors in $A[x]$ as the product of two monic polynomials $h(x) = f(x)g(x)$. Show that $f(x)$ and $g(x)$ are each in $R[x]$.

Hint: Consider the proof that an irreducible integer polynomial is irreducible over the rationals.

Proof: **PENDING:** yeah right. □

46 Integrality Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$. Show α is integral over $\mathbb{Z}$ if and only if $irr(\alpha;\mathbb{Q}) \in \mathbb{Z}[x]$.

Hint: Recall p
$\mathbb{Z}$ are irreducib
ever they are i

Proof: If $irr(\alpha;\mathbb{Q}) \in \mathbb{Z}[x]$ then by definition $irr(\alpha;\mathbb{Q})$ is monic and also $irr(\alpha;\mathbb{Q})(\alpha) = 0$ so indeed α is integral over $\mathbb{Z}$.

Now suppose instead that α is integral over $\mathbb{Z}$. Then there must exist a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Without loss of generality we may take $f(x)$ to be of the lowest possible degree with α as a root. Consequently, f is irreducible over $\mathbb{Z}$, so by Lemma-2.2.1 we know it to be irreducible over $\mathbb{Q}[x]$ as well and thus $f(x) = irr(\alpha;\mathbb{Q})$. $\square$

Hint: Follow the steps directly.

47 Integral Closure over $\mathbb{Z}$ For each $n \in \mathbb{Z}$ find the integral closure of $\mathbb{Z}[\sqrt{n}]$ as follows:

(i) Reduce to the case where n is square-free.

(ii) Use the fact that $\sqrt{n}$ is integral to deduce that what we want is the integral closure R of $\mathbb{Z}$ in the field $\mathbb{Q}(\sqrt{n})$.

(iii) If $\alpha = a + b\sqrt{n}$ with $a, b \in \mathbb{Q}$, deduce that the minimal polynomial of α is $x^2 - Tr(\alpha)x + N(\alpha)$, where $Tr(\alpha) = 2\alpha$ and $N(\alpha) = a^2 - b^2 n$. Thus, using Exercise-5.46, $\alpha \in R$ if and only if 2α and $a^2 - b^2 n$ are integers.

(iv) Show that if $\alpha \in R$ then $a \in \frac{1}{2}\mathbb{Z}$. If $a = 0$ show that $\alpha \in R$ if and only if $b \in \mathbb{Z}$. If $a = \frac{1}{2}$ and $\alpha \in R$, show that $b \in \frac{1}{2}\mathbb{Z}$; thus, subtracting a multiple of $\sqrt{n}$, we may assume $b = 0$ or $b = \frac{1}{2}$; $b = 0$ is impossible.

(v) Conclude that the integral closure is $\mathbb{Z}[\sqrt{n}]$ if $n \not\equiv 1 \pmod 4$, and $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{n}]$ otherwise.

Proof:

(i) If $n = a^2 m$ then $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}[\sqrt{m}]$ so without loss of generality we may assume n is square-free.

(ii) Notice that for any n, $x^2 - n \in \mathbb{Z}[x]$ so $\sqrt{n}$ is integral over $\mathbb{Z}[\sqrt{n}]$. So the integral closure can be agreed upon to lie within $\mathbb{Q}(\sqrt{n})$ – the field of fractions of $\mathbb{Z}[\sqrt{n}]$.

(iii) Given any $\alpha = a + b\sqrt{n} \in \mathbb{Q}(\sqrt{n})$ which is integral over $\mathbb{Z}[\sqrt{n}]$ it follows

$$(a + b\sqrt{n})^2 = a^2 + 2ab\sqrt{n} + b^2 n$$

so we eliminate all the terms with the monic polynomial:

$$p_\alpha(x) = x^2 - 2ax + a^2 - b^2 n = x^2 - Tr(\alpha)x + N(\alpha).$$

If the polynomial has smaller degree then $\alpha \in \mathbb{Z}[\sqrt{n}]$ to begin with. Therefore for any integral elements outside of $\mathbb{Z}[\sqrt{n}]$ we consider this to be precisely the minimal monic polynomial annihilating α. From Exercise-5.46 we know α is integral over $\mathbb{Z}[\sqrt{n}]$ if and only if $irr(\alpha;\mathbb{Q}(\sqrt{n}) \in \mathbb{Z}[\sqrt{n}][x]$.

(iv) So we set about verifying when the coefficients are in $\mathbb{Z}[\sqrt{n}]$. The term $2a \in \mathbb{Z}$ if and only if $a \in \frac{1}{2}\mathbb{Z}$. Also when $a = 0$ we see $b^2 n \in \mathbb{Z}$ so as $b \in \mathbb{Q}$ it follows $b \in \mathbb{Z}$ is required.

Suppose now $a = \frac{1}{2}$, then we require $\frac{1}{4} - b^2 n \in \mathbb{Z}$ so in fact $\frac{1}{2}$ divides b. Also, if $4|n - 1$ then

$$\frac{1}{4} - \frac{1}{4}n \in \mathbb{Z}.$$

So if $b = \frac{1}{2}$ then $n \equiv 1 \pmod 4$.

(v) So when $n \equiv 1 \pmod 4$ we may let $b = \frac{1}{2}$ and as such also let $a = \frac{1}{2}$ so we must adjoin this element to attain the closure:

$$\overline{\mathbb{Z}[\sqrt{n}]} = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{n}].$$

However when $n \not\equiv 1 \pmod 4$ then $a \neq 1/2$ and consequently $b \neq 1/2$. So indeed: $\overline{\mathbb{Z}[\sqrt{n}]} = \mathbb{Z}[\sqrt{n}]$.

□

48 Integral Closure of Non-UFDs Let $R = \mathbb{Z}[\sqrt{10}]$. Then R is integrally closed but R is not a UFD.

Hint: Use the norm function.

Example: We have seen before that the norm $N(a + b\sqrt{10}) = a^2 - 10b^2$ has the property that $N(xy) = N(x)N(y)$. Thus we notice as $N(2) = 4$ then if $2 = ab$ then $4 = N(ab) = N(a)N(b)$. So either one of a or b is a unit, or $N(a) = N(b) = \pm 2$. However this requires $2 = a_1^2 - 10a_2^2$. If we pass to $\mathbb{Z}/5$ any solution in $\mathbb{Z}$ must also produce a solution in $\mathbb{Z}/5$. Yet by empirical testing $2 \not\equiv a_1^2 \pmod 5$ for any a_1. Therefore there is no solution for this in $\mathbb{Z}$ either. Hence 2 is irreducible in R. The same procedure shows 3, $4 + \sqrt{10}$, and $4 - \sqrt{10}$ are also irreducible in R. However visibly

$$2 \cdot 3 = 6 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

Hence R is not a unique factorization domain.

Now we must demonstrate that R is yet integrally closed. Given that $10 \not\equiv 1 \pmod 4$ we know from Exercise-5.47 that $\mathbb{Z}[\sqrt{10}]$ is integrally closed. □

49 Prime Ideals of Integral Extensions

Hint: Notice the extension is an integral extension and that any ideal lying over $p\mathbb{Z}$ contains pR.

(i) Find all prime ideals of $\mathbb{Z}[\sqrt{5}]$ which lie over the prime ideal (5) of $\mathbb{Z}$.

(ii) Find all prime ideals of $\mathbb{Z}[\sqrt{5}]$ which lie over the prime ideal (3) of $\mathbb{Z}$.

(iii) Find all prime ideals of $\mathbb{Z}[\sqrt{5}]$ which lie over the prime ideal (2) of $\mathbb{Z}$.

Example: Notice that $\mathbb{Z}[\sqrt{5}]/\mathbb{Z}$ is an integral ring extension as $x^2 - 5$ is a monic polynomial annihilating $\sqrt{5}$. Therefore for each prime ideal P of $\mathbb{Z}$ there exists prime ideals P' of $\mathbb{Z}[\sqrt{5}]$ such that $P' \cap \mathbb{Z} = P$ – this by the going up theorem. Moreover by the maximality theorem we know all such P' are maximal in $\mathbb{Z}[\sqrt{5}]$ and moreover each is incomparable – as each prime ideal of $\mathbb{Z}$ is maximal.

Now it is clear that if $p\mathbb{Z} \subseteq P'$ where P' is a prime of $\mathbb{Z}[\sqrt{5}]$ laying over $p\mathbb{Z}$, then $p\mathbb{Z}[\sqrt{5}] \subseteq P'$.

Now suppose we consider $R = \mathbb{Z}[\sqrt{5}]$ and study R/pR for any prime $p \in \mathbb{Z}$. Clearly this yields the relation

$$a + b\sqrt{5} \equiv 0 \pmod{pR} \quad \Leftrightarrow \quad p|a \quad \text{and} \quad p|b.$$

Thus we have a suitably nice $\mathbb{Z}/p\mathbb{Z}$-algebra R/pR with center all $a + 0\sqrt{5}$. As any ideal of R/pR must also be a $\mathbb{Z}/p\mathbb{Z}$ vector space it follows $(\sqrt{5})/pR$ is the only option. Therefore this is both the Jacobson radical and the nil-radical. More importantly, it proves that pR is $(\sqrt{5})$-primary. Thus $\sqrt{pR}$ is the smallest prime ideal in R containing pR, and consequently $p\mathbb{Z}$. As $\sqrt{pR}$ is also maximal (see the above argument) it is the unique prime ideal of R laying over $p\mathbb{Z}$. Now we switch to specific examples.

(i) As $R5\mathbb{Z} = 5R$ it follows every ideal over $5\mathbb{Z}$ contains $5R$. Now the radical $\sqrt{5R} = \sqrt{5}R$. Since $\sqrt{5}R$ is maximal – its quotient is $\mathbb{Z}/5\mathbb{Z}$ – it is prime. Moreover, as it is a maximal prime, which by definition of begin a radical ideal, contains all primes that contain $5R$, it is the unique prime ideal over $5\mathbb{Z}$.

(ii) For $p = 3$ consider $R/3R$.

$$R/3R = \{0, 1, 2, \sqrt{5}, 2\sqrt{5}, 1 + \sqrt{5}, 1 + 2\sqrt{5}, 2 + \sqrt{5}, 2 + 2\sqrt{5}\}.$$

By testing we see for all $n \neq 0$:

$$1 \equiv n^4 \equiv (n\sqrt{5})^4 \equiv (n(1 + \sqrt{5}))^8 \equiv (n(1 + 2\sqrt{5}))^8 \pmod{3R}.$$

Therefore $R/3R$ is the field $\mathbb{F}_9$. Hence $3R$ is maximal and so prime and also by the fact that $R(3\mathbb{Z}) = 3R$ and the maximality theorem, it is the unique prime ideal lying over $3\mathbb{Z}$.

(iii) For $p = 2$ the procedure is the same. Consider $R/2R$. Here we get the elements 0, 1, $\sqrt{5}$, and $1 + \sqrt{5}$. Notice that the only nilpotent elements are 0 and $1 + \sqrt{5}$ so they form the nil-radical.

$$\begin{array}{c} R/2R \\ | \\ (1+\sqrt{5})/2R \\ | \\ \mathbf{0} \end{array}$$

As the quotient has all zero-divisors as nilpotent elements it follows $2R$ is $(1+\sqrt{5})R$-primary. As the radical of a primary ideal is the smallest prime ideal containing the ideal, and this radical is also maximal, it follows it is the unique prime ideal in R lying over $2\mathbb{Z}$.

□

Hint: Show I times the product of all but one prime lies in this left out prime ideal.

50 Prime Unions Let $P_1, \ldots, P_r$ be prime ideals of a commutative ring. Show that an ideal I which is contained in $P_1 \cup \cdots \cup P_r$ is contained in some P_i.

Proof: Suppose I is not contained completely in any P_i. So without loss of generality assume $I \cap P_i \neq \mathbf{0}$ for any i – if it does we can remove this P_i from the union. Therefore we know P_i is not contained in P_j for any $i \neq j$.

If $J = I \cap \bigcap_{i \neq j} P_i$ is not contained in P_j for every j, then pick $x_j \in J \backslash P_j$. Notice then $x_1 + \cdots + x_r \in I \backslash (P_1 \cup \cdots \cup P_r)$. Yet I lies in $P_1 \cup \cdots \cup P_r$ so indeed there exists a j for which $I \cap \bigcap_{i \neq j} P_i$ is contained in P_j. But this means $I \prod_{i \neq j} P_i \subseteq P_j$ so that $I \subseteq P_j$ as P_j is prime. □

Hint: The associated primes of an ideal in a noetherian ring are unique.

51 Primary Decomposition Let I be a an ideal of a noetherian ring R with a reduced primary decomposition $I = Q_1 \cap \cdots \cap Q_r$. Show that every prime ideal of R which is minimal over I is the radical of some Q_i. Is the converse true?

Proof: We know the associated primes $\sqrt{Q_i}$ are the unique □

Hint:

52 Prime Height Let P be a prime ideal of height r in a noetherian ring R. Show that there exists an ideal I of R with r generators over which P is minimal.

Proof:
□

53 Krull Dimension Let P be a prime ideal of R. Show that the height of P is the dimension of R_P.

Hint: Recall there is a bijection between the prime ideals of the local ring and the primes below the prime of localization.

Proof: Let $\{P_i : i \in I\}$ be a be a chain of primes of maximum length below P – we assume the length if finite as the height is assumed to exist. Then we know that R_P has unique maximal ideal P_P and because each prime below P_P there is a one-to-one correspondence with primes below P in R we see that $\{P_{iP} : i \in I\}$ is a maximum length chain of primes below P_P.

Since R_P is a local ring, any chain of primes can be augmented to begin from P_P and as such the Krull dimension of R_P will be determined by the longest descending chain of primes from P_P. As we have seen this chain has the same length as the height of P in R so the two invariants agree. □

54 Krull Dimension Let P be a non-zero prime ideal of R. Show that $dim\ R \geq 1 + dim\ R/P$.

Hint: Notice the pre-image, under a surjective map, of prime ideals is prime.

Proof: First we resolve a simple lemma: let $\pi : R \to R/P$ and take any prime Q of R/P. Then $\pi^{-1}(Q)$ is prime in R. To see this notice

$$R/\pi^{-1}(Q) \cong \frac{R/P}{\pi^{-1}(Q)/P} \cong \frac{R/P}{Q},$$

by the second isomorphism theorem. Since Q is prime in R/P, the quotient is an integral domain and therefore so is $R/\pi^{-1}(Q)$. Hence we may say $\pi^{-1}(Q)$ is prime in R.

Now take a maximum length chain of descending primes in R/P – which we assume to exist as the Krull dimension is defined.

$$Q_0 > Q_1 > \cdots > Q_m.$$

We pull the chain back to R by the correspondence theorem and find

$$\pi^{-1}(Q_0) > \pi^{-1}(Q_1) > \cdots > \pi^{-1}(Q_m) \geq P > \mathbf{0}.$$

Therefore we have a chain in R of primes of length at least $m+1$. So we must conclude

$$dim\ R \geq 1 + dim\ R/P.$$

□

55 Minimal Primes Let F be an algebraically closed field. Show that the minimal prime ideals of $F[x_1, \ldots, x_n]$ are the principal ideals generated by irreducible polynomials.

Hint: Consider the associated varieties of the minimal prime ideals.

Proof: Given any minimal prime ideal P, we know $\sqrt{P} = P$ so we may pass to the variety without loss of information. As P is minimal in $R = F[x_1, \ldots, x_n]$ and Z is an order reversing bijection of varieties and radical ideals – to follows $Z(P)$ is maximal in the set of all varieties (under set inclusion.)

As R is noetherian there are finitely many generators fo P call them $f_1, \ldots, f_n$ and none of them trivial. Suppose further that $f_i \neq f_j$ for some i, j. Then $Z(f_i) \neq Z(f_j)$ and so $Z(P) \subseteq Z(f_i) \cap Z(f_j)$. But as $Z(P)$ is maximal this cannot be so we admit $f_1 = \cdots = f_n$ so $P = (f_1)$. Furthermore, if $f_1 = g \cdot h$ then as P is prime it contains either g or h and so f_1 does not generate P. Therefore we see f_1 is irreducible.

Now take any irreducible polynomial $f \in F[x_1, ;x_n]$ and consider (f). Given $gh \in (f)$ it follows $f|gh$ so either $f|g$ or $f|h$ as R is a UFD. Thus (f) is a prime ideal of R. Furthermore it is a minimal prime because it does not divide other irreducibles to which it is not associate. $\square$

Hint: Choose the generators of $I(Z(S))$.

56 Generators of Varieties – True or False? Let F be a field. If S is an arbitrary subset of $F[x_1, \dots, x_n]$, then there is a finite subset T of $F[x_1, \dots, x_n]$ such that $Z(S) = Z(T)$.

Proof: True. **PENDING:** determine if algebraically closed matters. As every field is noetherian so is $F[x_1, \dots, x_n]$. Furthermore, for every subset S there is associated a radical ideal $I = I(Z(S))$. As every ideal in a noetherian ring is finitely generated let T be the generators of I. Clearly then $Z(S) = Z(I) = Z(T)$. $\square$

Hint: Use the Nullstellensatz.

57 Non-radical Ideals – True or False? Let F be a field. If I is any ideal of $F[x_1, \dots, x_n]$, then $I = \{f \in F[x_1, \dots, x_n] \ : \ f(a) = 0 \text{ for each } a \in Z(I)\}$.

Example: False. Let $F = \mathbb{C}$. Then we have the Nullstellensatz which state $I(Z(I)) = \sqrt{I}$. So let $n = 1$ and take $I = (x^2)$. Clearly then $I(Z(I)) = (x) \neq (x^2)$. $\square$

Hint: Note that $IJ \subseteq I \cap J$.

58 Ideal Lattice and Varieties – True or False? Let F be algebraically closed and I, J be ideals in $F[x_1, \dots, x_n]$. Then $Z(I) \cup Z(J) = Z(IJ)$.

Proof: True. An element $a \in F^n$ is in $Z(IJ)$ if and only if $f(a)g(a) = 0$ for all $f \in I$ and $g \in J$ which happens precisely when either $f(a) = 0$ or $g(a) = 0$ for each pair $f \in I, g \in J$. That is if and only if $a \in Z(I)$ or $a \in Z(J)$. Therefore $Z(I) \cup Z(J) = Z(IJ)$. $\square$

Hint: Recall if P is prime containing IJ then it contains I or J.

59 Radical Ideals – True or False? Let F be a field, and I, J be ideals in $F[x_1, \dots, x_n]$. Then $\sqrt{I \cap J} = \sqrt{IJ}$.

Proof: It is clear the $IJ \subseteq I \cap J$ so $\sqrt{IJ} \subseteq \sqrt{I \cap J}$. Now consider the reverse inclusion.

Let P be a prime lying over IJ. It follows either $I \leq P$ or $J \leq P$ as P is prime. In either case $I \cap J \leq P$. So we conclude:

$$\sqrt{IJ} = \bigcap_{IJ \subseteq P} P = \bigcap_{I \cap J \leq P} P = \sqrt{I \cap J}.$$

$\square$

Hint: Notice if $\sqrt{I+J} = A$ then $1^n \in I+J$ so $I+J = A$.

60 Direct Products with Varieties Let I and J be ideals of $A = \mathbb{C}[x, y]$ and $Z(I) \cap Z(J) = \varnothing$. Show that $A/(I \cap J) \cong A/I \times A/J$.

Proof: We begin with the given:

$$Z(I + J) = Z(I) \cap Z(J) = \varnothing.$$

Then we apply the Nullstellensatz:

$$\sqrt{I + J} = I(Z(I + J)) = I(\varnothing) = A.$$

Now that $1 \in \sqrt{I + J}$ it follows that $1^n = 1 \in I + J$ for some n. However this implies $I + J = A$. Therefore we have all the ingredients of a split extension:

both I and J are ideals, their join is A so when we quotient by $I \cap J$ then we have our split:

$$\begin{tikzcd}[column sep=small] & I+J/(I\cap J) \arrow[dl, dash] \arrow[dr, dash] & \\ I/(I\cap J) \arrow[dr, dash] & & J/(I\cap J) \arrow[dl, dash] \\ & (I\cap J)/(I\cap J) & \end{tikzcd}$$

Thus we have by the third isomorphism theorem:

$$A/(I \cap J) \cong I/(I \cap J) \times J/(I \cap J) \cong A/J \times A/I.$$

□

61 DCC for Varieties – True or False? Let F be algebraically closed. Any decreasing sequence of algebraic sets in F^n stabilizes.

Hint: Use the noetherian property of $F[x_1, \ldots, x_n]$.

Proof: True. Let

$$Z_1 \geq Z_2 \geq \cdots$$

be a decreasing sequence of varieties. Then as F is algebraically closed we may use the Nullstellensatz to produce an identical length chain

$$I(Z_1) \leq I(Z_2) \leq \cdots$$

in $F[x_1, \ldots, x_n]$. However here we have an ascending chain of ideals in a noetherian ring so it must stabilize, say $I(Z_n) = I(Z_m)$ for all $n > m$. Now we reapply the Nullstellensatz to see:

$$Z_n = Z(I(Z_n)) = Z(I(Z_m) = Z_m$$

so the descending chain of varieties stabilizes in F^n. □

62 ACC for Varieties – True or False? Let F be algebraically closed. Any increasing chain of algebraic sets in F^n stabilizes.

Hint: Consider the chain of zeros $\{0\}, \{0, 1\}, \ldots$

Example: False. Consider the descending chain of ideals

$$(x) \geq (x(x-1)) \geq (x(x-1)(x-2)) \geq \cdots$$

in $\mathbb{C}[x]$. Immediately we see the associated variety chain:

$$Z(x) = \{0\} \subsetneq Z(x(x-1)) = \{0, 1\} \subsetneq Z(x(x-1)(x-2)) = \{0, 1, 2\} \subsetneq \cdots$$

ascends forever never stabilizing. □

63 ACC for Varieties – True or False? Let F be algebraically closed. Any increasing sequence of irreducible algebraic sets in F^n stabilizes.

Hint: Consider the Krull dimension of of the varieties.

Proof: True. Given any chain of irreducible varieties

$$Z_1 \leq Z_2 \leq \cdots$$

it follows the associated ideals are all prime so we get

$$P_1 = I(Z_1) \leq P_2(Z_2) \leq \cdots$$

However if we take $P = \bigcup_i I(Z_i)$ we get a prime under which is a chain of primes. Since $F[x_1, \ldots, x_n]$ is noetherian, Krull's finite height theorem tells us that this chain of primes can only have finite length. Therefore the chain must stabilizes, say $P_i = P_j$ for all $j > i$. Now reapply the Nullstellensatz:

$$Z_i = Z(I(Z_I)) = Z(P_i) = Z(P_j) = Z(I(Z_j)) = Z_j.$$

Therefore an ascending chain of irreducibles must stabilize. □

Hint: Consider the variety spanned by all f_i.

64 Solution Sets and Varieties – True or False? Let F be an algebraically closed field. A system of polynomial equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

over F has no solutions in F^n if and only if 1 can be expressed as a linear combination $1 = \sum_i p_i f_i$ with polynomial coefficients p_i.

Proof: True Let $I = (f_1, \ldots f_m)$.

Suppose the system has no solutions, that is: $Z(I) = \varnothing$. As F is algebraically closed we use the Nullstellensatz to say

$$\sqrt{I} = I(Z(I)) = I(\varnothing) = F[x_1, \ldots, x_n].$$

As such, $1 \in \sqrt{I}$ so $1^n = 1 \in I$ for some n, so indeed $I = F[x_1, \ldots, x_n]$. As $I = (f_1, \ldots, f_n)$ it clear that $1 = \sum_i g_i f_i$ for appropriate g_i.

Now suppose that 1 is not a linear combination of the f_i's. It follows I is a proper ideal and so $Z(I) \neq emptyset$. But as $Z(I)$ is the set of all solutions to the system we see there are in fact solutions to the system now. □

Hint: The basic closed sets in $\mathbb{C}$ are finite subsets of $\mathbb{C}$ while $\mathbb{C}^2$ includes the uncountably infinite lines.

65 Zariski Topology – True or False? The Zariski topology on F^{m+n} is the product topology of the Zariski topologies on F^n and F^m.

Example: False. The product topology has too few closed sets. For instance, consider $F = \mathbb{C}$ and $n = m = 1$. In $\mathbb{C}$ the varieties are all finite subsets of $\mathbb{C}$. For $\mathbb{C}^2$ the varieties also include such things as the line through $y - x$ which when projected in $\mathbb{R}$ is $y = x$ – clearly an uncountably infinite set of points. However if $\mathbb{C}^2$ where to have the same Zariski topology as $\mathbb{C} \times \mathbb{C}$ then this line – a closed set in $\mathbb{C}^2$ – would have to be the finite union of basic closed sets in $\mathbb{C} \times \mathbb{C}$. The basic sets in $\mathbb{C} \times \mathbb{C}$ are all products of finite subsets which are clearly always finite. Thus the task is impossible. □

Hint:

66 Zariski Topology Let R be any ring. Denote by $Spec\ R$ the set of the prime ideals of R. For any ideal $I \trianglelefteq R$ denote

$$Z(I) := \{P \in Spec\ R\ :\ I \leq P\}.$$

Introduce the Zariski topology on $Spec\ R$ by declaring the sets of the form $Z(I)$ to be closed. Define a *distinguished open set* of $Spec\ R$ to a set of the form

$$U(f) := \{P \in Spec\ R\ :\ f \notin P\}$$

where $f \in R$.

(a) Prove that this is indeed a topology.

(b) Prove that distinguished opens sets are indeed open, and moreover, they form a basis of the Zariski topology. Show that $Spec\ R = \bigcup_i U(f_i)$ for some collection f_i of elements of R if and only if the ideal generated by all the f_i's is R.

(c) Prove that $Spec\ R$ is compact in the Zariski topology.

Proof: **PENDING:** when pigs fly and quals pass. □

67 Zariski Topology and Frobenius – True or False? Let F be an algebraically closed field of characteristic $p > 0$, and $Fr : F \to F : a \mapsto a^p$ be the Frobenius homomorphism. True or False: **Hint**:

(i) Fr is a homeomorphism in the Zariski topology.

(ii) Fr is an isomorphism of algebraic sets.

(i) **Proof:** True.
□

(ii) **Example:**
□

68 Automorphisms of Varieties Describe all automorphism of the algebraic set F. **Hint**:

Example:
□

69 Isomorphism of Varieties Which of the following algebraic sets over $\mathbb{C}$ are isomorphic. **Hint**:

(i) $\mathbb{C}$;

(ii) $Z(x) \subset \mathbb{C}^2$;

(iii) $Z(y - x^2) \subset \mathbb{C}^2$;

(iv) $Z(y^2 - x^3) \subset \mathbb{C}^2$;

(v) $Z(y^2 - x^3 - x^2) \subset \mathbb{C}^2$.

Example:
□

Bibliography

[Hun74] Thomas W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[Kle03] Alexander Kleshchev, *Lectures on abstract algebra for graduate students*, pre-print, University of Oregon, Eugene, Oregon, 2003.

[Rot02] Joseph J. Rotman, *Advanced modern algebra*, Prentice Hall, Upper Saddle River, New Jersey, 2002.

Index