Mathematics 504 Autumn 2003

1. Show that any finite abelian group is isomorphic to the direct product of its Sylow subgroups (without using the fundamental theorem of finitely generated abelian groups).

Solution. We proceed by induction on the number of prime factors in the order of the group. If G has order p^n for some prime p and integer n, then G equals its Sylow p-subgroup, so is trivially the product of its Sylow subgroups.

Assume that any abelian group with fewer than m distinct prime factors is isomorphic to the product of its Sylow subgroups, and let G be abelian with $|G| = p_1^{i_1} \dots p_m^{i_m}$ with the p_j's distinct primes.

Let H be the subgroup of G generated by the Sylow p_j-subgroups, for $1 \leq j \leq m-1$. Since G is abelian, every element of H has order prime to p_m: H is generated by elements of order p_j^k for $1 \leq j \leq m-1$, and the order of the product of commuting elements is the least common multiples of the orders of the factors. Thus the elements of H have order dividing $p_1^{i_1} \cdots p_{m-1}^{i_{m-1}}$. Because H has as subgroups the Sylow p_j-subgroups of G, its order must be at least $p_1^{i_1} \dots p_{m-1}^{i_{m-1}}$. Since $|H|$ divides $|G|$ and since H has no elements of order p_m^k for any k, the order of H must be exactly $p_1^{i_1} \dots p_{m-1}^{i_{m-1}}$. By induction, then, this subgroup is isomorphic to the product of its Sylow subgroups:

$$H \cong P_1 \times \cdots \times P_{m-1},$$

where P_j is the Sylow p_j-subgroup. Now consider H together with P_m, the Sylow p_m-subgroup. Since G is abelian, each of these subgroups is normal. By order considerations, the intersection of these subgroups is $\{1\}$ – every element in P_m has order p_m^i for some i, while all the elements in H (except for 1) have order prime to p_m. Finally, a counting argument shows that $HP_m = G$: the elements $\{hk : h \in H,\ k \in P_m\}$ are distinct, and this set has size $|G|$.

Thus by the recognition theorem for direct products,

$$\begin{aligned} G &\cong H \times P_m \\ &\cong P_1 \times \cdots \times P_{m-1} \times P_m. \end{aligned}$$

---

2. If K/F is an abelian Galois extension of degree $540 = 2^2 \times 3^3 \times 5$, what are the possible Galois groups? Among all such extensions, what is the maximum number of intermediate fields E such that $[K : E] = 2$? What is the minimum number?

Solution. By the fundamental theorem for finitely generated abelian groups, the possible Galois groups are:

$$\begin{array}{cc} C_4 \times C_{27} \times C_5, & C_2 \times C_2 \times C_{27} \times C_5, \\ C_4 \times C_9 \times C_3 \times C_5, & C_2 \times C_2 \times C_9 \times C_3 \times C_5, \\ C_4 \times C_3 \times C_3 \times C_3 \times C_5, & C_2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_5. \end{array}$$

Next, according to the fundamental theorem of Galois theory, the intermediate fields E with $[K : E] = 2$ are in bijection with subgroups of order 2 of the Galois group. Any subgroups of order 2 of the Galois group will be contained in the Sylow 2-subgroup, which is either C_4 or $C_2 \times C_2$, so it

suffices to count the number of subgroups of order 2 in each of these groups. $C_4 = \{1, a, a^2, a^3\}$ has a unique subgroup of order 2: $\{1, a^2\}$. $C_2 \times C_2 = \{1, a, b, ab\}$ has 3 subgroups of order 2: $\{1, a\}$, $\{1, b\}$, $\{1, ab\}$. So the maximum number is 3, and the minimum number is 1.

---

3. Assume that G is a group of order $231 = 3 \times 7 \times 11$. Show that G contains a normal Sylow 7-subgroup and a central Sylow 11-subgroup.

Solution. According to the Sylow theorems, n_3 is congruent to 1 mod 3, and divides 77; thus n_3 is either 1 or 7. n_7 is congruent to 1 mod 7 and divides 33, and so equals 1. n_{11} is congruent to 1 mod 11 and divides 21, and so equals 1. Thus there is a normal Sylow 7-subgroup and a normal Sylow 11-subgroup.

Let P be the normal Sylow 11-subgroup. P is isomorphic to C_{11}; let x be a generator.

To show that P is central, it suffices to show that x commutes with every element of G. The map $g \longmapsto gxg^{-1}$ sends each group element g to an automorphism of $P = C_{11}$; in other words, this defines a group homomorphism $G \to \mathrm{Aut}(C_{11})$. $\mathrm{Aut}(C_{11})$ is isomorphic to C_{10}. The order of the image of G must divide 10, and also must divide the order of G; thus the image of G must be 1: every element of g maps to the identity automorphism. That is, for all $g \in G$, $gxg^{-1} = x$, so x is central, and so P is central.

---

4. Let p be a prime and n a positive integer. Use the fundamental theorem of Galois theory and facts about the extension $\mathbf{F}_{p^n}/\mathbf{F}_p$ to classify the subfields of $\mathbf{F}_{p^n}$.

Solution. Every subfield of $\mathbf{F}_{p^n}$ must contain 1, and so must contain the prime field $\mathbf{F}_p$. Thus the subfields of F_{p^n} are precisely the intermediate fields in this extension. The extension $\mathbf{F}_{p^n}/\mathbf{F}_p$ is Galois, with Galois group $G \cong C_n$, generated by the Frobenius φ. The subgroups of C_n are the groups C_d, generated by φ^d, for each divisor d of n.

According to the fundamental theorem of Galois theory, there is a bijection between the subgroups of the Galois groups and the intermediate fields, sending a subgroup H to its fixed field. The order of the group equals the degree of the big field over the fixed field. So in our case, C_d corresponds to a field F so that $[\mathbf{F}_{p^n} : F] = d$, which means that F has $p^{n/d}$ elements. Finite fields are unique up to isomorphism, so F must be $\mathbf{F}_{p^{n/d}}$.

So the subfields of $\mathbf{F}_{p^n}$ are the fields $\mathbf{F}_{p^d}$, for all divisors d of n.

---

5. Let F be a field and let $p(x)$ be an irreducible polynomial in $F[x]$. Let K be the splitting field of $p(x)$. Show that the Galois group $G = \mathrm{Gal}(K/F)$ acts transitively on the roots of $p(x)$. (For full credit, do this without using the fundamental theorem of Galois theory.)

Solution. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $p(x)$. Since G fixes the field F, G fixes the coefficients of $p(x)$, and so for any element σ of G, σ permutes the roots of $p(x)$. (For any element c of F, $\sigma(p(c)) = p(\sigma(c))$. So if $p(c) = 0$, then $\sigma(p(c)) = 0$, so $p(\sigma(c)) = 0$. That is, if c is a root, so is $\sigma(c)$.)

Let $\beta_1 = \alpha_1, \beta_2, \ldots, \beta_m$ be the distinct Galois conjugates of α_1. Then I claim that

$$h(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_m)$$

is fixed by the action of G: for any i, $\beta_i = \sigma_i\alpha_1$ for some $\sigma_i \in G$, so for any $\tau \in G$,

$$\tau(\beta_i) = (\tau\sigma_i)\alpha_1 = \sigma_j\alpha_1 = \beta_j$$

for some j. So G acts on $h(x)$ by permuting the factors, and so $h(x)$ is fixed by G. Thus $h(x) \in F[x]$, and it has α_1 as a root. Note also that $h(x)$ divides $p(x)$, since the roots of $h(x)$ form a subset of the roots of $p(x)$. On the other hand, $p(x)$ has coefficients in F and has α_1 as a root, and $p(x)$ is irreducible; thus $p(x)$ must be the minimal polynomial for α_1. By uniqueness of minimal polynomials, $p(x)$ must divide $h(x)$. Since $p(x)$ and $h(x)$ divide each other, they must be scalar multiples of each other, and so all of the roots of $p(x)$ are actually roots of $h(x)$: every α_i is a Galois conjugate of α_1.

---

6. Let K/F be a field extension, and fix $a \in K$. Show that $F(a)$ is algebraic over F if and only if $[F(a):F]$ is finite. Use this to prove that sums, differences, products, and quotients of algebraic elements are algebraic.

Solution. If $F(a)/F$ is algebraic, then the element a is algebraic over F, and so it satisfies some polynomial

$$g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in F[x].$$

Thus a^n can be written in terms of smaller powers of a, and by induction, for any $m \geq n$, a^m can be written in terms of $1, \ldots, a^{n-1}$. Thus the elements $\{a^j : 0 \leq j \leq n-1\}$ span $F(a)$, and so $[F(a):F] \leq n$. (Alternatively, if we assume that $g(x)$ is the minimal polynomial for a, then $F(a) \cong F[x]/(g(x))$, which is an n-dimensional vector space over F.)

Conversely, suppose that $[F(a):F]$ is finite. For any $b \in F(a)$, the elements $1, b, b^2, b^3, \ldots$ cannot be linearly independent – there must be some number n and some elements $c_i \in F$ so that

$$c_nb^n + c_{n-1}b^{n-1} + \cdots + c_1b + c_0 = 0$$

Thus b is a root of the polynomial $f(x) = c_nx^n + \cdots + c_0 \in F[x]$, which means that b is algebraic. This holds for any $b \in F(a)$, and thus $F(a)$ is algebraic over F.

Now given an extension K/F and two elements a and b of K which are algebraic over F, then I claim that $[F(a,b):F]$ is finite. First note that $F(a,b) = F(a)(b)$. b satisfies a polynomial with coefficients in F, and I can view the same polynomial as having coefficients in $F(a)$, and thus b is algebraic over $F(a)$, so $[F(a)(b):F(a)]$ is finite. a is algebraic over F, so $[F(a):F]$ is finite. By multiplicativity of degrees of field extensions, $[F(a,b):F] = [F(a,b):F(a)][F(a):F]$ is finite. Thus every element in $F(a,b)$ is algebraic over F: for any $c \in F(a,b)$, $[F(c):F]$ divides $[F(a,b):F]$, hence is finite, and hence c is algebraic. The field $F(a,b)$ contains $a+b$, $a-b$, ab, and (if b is nonzero) $ab^{-1} = a/b$; and so all of these elements are algebraic.

---

7. Suppose that $f(x)$ is a degree 4 polynomial with coefficients in a field F, and let K be the splitting field of $f(x)$. What are the possible values for $[K:F]$? Give examples for as many of those values as you can. (You should be able to do more than half of the possibilities; I will be impressed if you can find examples for all of them.)

Solution. $[K:F]$ must divide $4! = 24$, so the possible values are 1, 2, 3, 4, 6, 8, 12, and 24. Here are examples:

1. For any field F, x^4 splits over F, and so $K = F$ and $[K:F] = 1$.

2. Let $F = \mathbf{Q}$. Then $x^2(x^2-2)$ does not split completely over $\mathbf{Q}$ (because $\sqrt{2} \notin \mathbf{Q}$), but it does split over $\mathbf{Q}(\sqrt{2})$. Thus $K = \mathbf{Q}(\sqrt{2})$, and $[K:F] = 2$.

3. Let $F = \mathbf{F}_2$, for a change of pace. The polynomial $p(x) = x^3 + x + 1 \in \mathbf{F}_2[x]$ is irreducible, so $x(x^3+x+1)$ does not split over $\mathbf{F}_2$. $p(x)$ does have a root in $\mathbf{F}_8 \cong \mathbf{F}_2[x]/(p(x))$, and since $\mathbf{F}_8/\mathbf{F}_2$ is Galois, once an irreducible polynomial has one root in $\mathbf{F}_8$, it splits completely there. So the splitting field is $\mathbf{F}_8$, which has degree 3 over $\mathbf{F}_2$.

4. Let $F = \mathbf{Q}$. Then the splitting field of $(x^2-2)(x^2-3)$ is $\mathbf{Q}(\sqrt{2},\sqrt{3})$. The biquadratic extension $Q(\sqrt{2},\sqrt{3})/\mathbf{Q}$ has degree 4.

24. Let L be a field, let $K = L(x_1,x_2,x_3,x_4)$, and let $F = L(s_1,s_2,s_3,s_4)$, where s_i is the ith elementary symmetric polynomial in $x_1, \ldots, x_4$. Then

$$(x-x_1)(x-x_2)(x-x_3)(x-x_4)$$

lies in $F[x]$, and its splitting field is K. The degree of K over F is $4! = 24$.

I thought of those examples first. Here are some other ones:

6. One easy way to do this: find an irreducible degree 3 polynomial with Galois group S_3 and multiply it by x. For example, I could imitate the degree 24 case and look at $x(x-x_1)(x-x_2)(x-x_3)$ in $L(s_1,s_2,s_3)[x]$. Alternatively, I could explain why $x^3-2 \in \mathbf{Q}[x]$ has Galois group S_3 (its splitting field is $\mathbf{Q}(\sqrt[3]{2},\zeta)$ where ζ is a primitive cube root of unity), and look at $x(x^3-2)$.

8. We did one like this in class: let $F = \mathbf{Q}$ and look at x^4-2. Then its splitting field is $\mathbf{Q}(2^{1/4},i)$, which has degree 8 over $\mathbf{Q}$.

12. For this one, I need a polynomial whose Galois group is isomorphic to A_4. This is harder to come up with off the top of my head. I guess a cheap way to do it would be to modify the degree 24 case: let L be a field, let $K = L(x_1,x_2,x_3,x_4)$, and let $F = L(s_1,s_2,s_3,s_4)$, where s_i is the ith elementary symmetric polynomial in $x_1, \ldots, x_4$. Then K/F is Galois with Galois group S_4, so let E be the fixed field of the subgroup $A_4 \leq S_4$. Then $[K:E] = |A_4| = 12$, and K is the splitting field of the polynomial

$$(x-x_1)(x-x_2)(x-x_3)(x-x_4),$$

which I can view as lying in $E[x]$. (I could have done lots of these examples this way, I suppose...)