1

2

Dummit and Foote
page 530, problems 4,12,13,14,16,17
Notation. $\mu_n(R) = \{x \in R : x^n = 1\}$ where R is a commutative ring and n is a natural number. Note that $\mu_n(R)$ is a sugroup of $R^\times$, the group of units of R.
Theorem proved in class F is a field, n is a natural number. Assume that the order of group $\mu_n(F)$ is n. Let $0 \neq a \in F$. Let $E = F(\alpha)$ where $\alpha^n = a$. Let $d = \deg(E/F)$.Then
(1)d divides n. There is some $b \in F$ such that $b^{\frac{n}{d}} = a$ and $\alpha^d = b$.
(2) Let $\beta \in E$. Assume that $\beta^d \in F$.Then $\beta^d = b^k c^d$ for some $k \in \mathbb{Z}\, c \in F$.
The problems below use only the easy case $n = 2$ of the above theorem

2.1. Let F be a field of characteristic $\neq 2$ and let E be a quadratic extension of F. Show that the kernel of the natural homomorphism $F^\times/(F^\times)^2 \to E^\times/(E^\times)^2$ is a group of order 2.

Deduce that if there is a chain of fields $F = E_0 \subset E_1 \subset ... \subset E_n = E$ with $\deg(E_i/E_{i-1}) = 2$ for $i = 1, 2, ..., n$, then the kernel of the natural homomorphism $F^\times/(F^\times)^2 \to E^\times/(E^\times)^2$ has order dividing 2^n.

2.2. Char.F is $\neq 2$. Let $a_1, a_2, ..., a_r$ be nonzero elements of F and let G be the subgroup generated by their images in $F^\times/(F^\times)^2$. Let $E = F(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_r})$. Prove that $\deg(E/F)$ is the order of G.

2.3. Here $(a_1, a_2, a_3) = (2, 3, 5)$. Let $E = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$. Let $(b_1, b_2, b_3) \in \{\pm 1\}^3$. Prove

(1) There exists a field automorphism σ of E such that $\sigma\sqrt{a_i} = b_i\sqrt{a_i}$ for $i = 1, 2, 3$.
Hint: Use the previous problem to do this when (b_1, b_2, b_3) equals $(1, 1, -1), (1, -1, 1), (-1, 1, 1)$, and then consider the group generated by these three automorphisms.
(2) Deduce that $\mathbb{Q}(\sqrt{a_1} + \sqrt{a_2} + \sqrt{a_3}) = E$.
Hint: First deduce from part (1) that $\pm\sqrt{a_1} + \pm\sqrt{a_2} + \pm\sqrt{a_3}$ are all conjugates of each other.

2.4. Let $x_1, x_2, x_3 \in F$. Find a monic degree eight $f \in F[X]$ which has $\sqrt{x_1} + \sqrt{x_2} + \sqrt{x_3}$ as a root.

3

3.1. p is an odd prime and $q = p^k$. Let E be a splitting field of $X^q + X \in \mathbb{F}_p[X]$.How many elements does it have?

3.2. For which primes p is there some $1 \neq \omega \in \mathbb{F}_p$ such that $\omega^3 = 1$. For such a prime p, how many elements are there in a splitting field of $X^p - \omega X \in \mathbb{F}_p[X]$

3.3. Let p be a prime which is $\equiv 1 \bmod 2^k$, but not congruent to 1 modulo a higher power of 2. Assume $k \geq 2$. Assume that $u_0 \in \mathbb{F}_p$ is not a square. Construct a sequence of pairs (E_n, u_n) where E_n is a field and $u_n \in E_n$ as follows.
Define $(E_0, u_0) = (\mathbb{F}_p, u_0)$.

Assume that (E_n, u_n) has been defined. Let E_{n+1} be a field extension of E_n obtaing by adjoining a square-root u_{n+1} of $u_n \in E_n$.

Show that $\deg(E_n/E_{n-1}) = 2$ for all $n > 0$.

3.4. Explain how you would construct a sequence of quadratic extensions when $k = 1$ in the previous problem.

3.5. Explain how you would obtain a sequence of field extensions E_{n+1}/E_n of degree three, with $E_0 = \mathbb{F}_{19}$.

3.6. Let $\mathbb{F}_q$ be a finite field of characteristic p. How mny elements of $\mathbb{F}_q$ are of the type $x - x^p, x \in \mathbb{F}_q$?

3.7. The cylotomic polynomials $\Phi_n(X) \in \mathbb{Z}[X]$ defined for all natural numbers n, have the property

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Let $n = n'p^k$ with p not dividing n'. let F be a field of characteristic p such that $\mu_{n'}(F)$ has order n'. Show that the roots of $\Phi_n(X)$ in F are the primitive n'-th roots of unity, each of them occuring with multiplicity $\varphi(p^k)$.
Here φ is Euler's phi function.
$\varphi(m)$ is the order of the group of units of the ring $\mathbb{Z}/m\mathbb{Z}$.
Equivalently, $\varphi(m)$ is the cardinality of the set of natural numbers $k \leq m$ such that g.c.d.$(k, m) = 1$.
$\varphi(1) = 1$. If p is a prime, then $\varphi(p^k) = p^{k-1}(p-1)$ if $k > 0$.

3.8. Deduce the equality $\Phi_n(X) = \Phi_{n'}(X)^{\varphi(p^k)}$ in $\mathbb{F}_p[X]$ from the previous problem.

3.9. Let $f = Q^2 - cP^2$ where $c \in F$ and $P, Q \in F[X]$ with Q monic of degree two and $\deg(P) < 2$. Show that if g is an irreducible monic polynomial of degree ≥ 3 that divides f, then $g = f$.

Show that if f is irreducible, then the field $E = F(\theta)$ obtained by adjoining a root θ of f, necessarily contains a quadratic extension of F

3.10. Conversely, Let $E = F(\theta)$ be a edgree four extension of F that contains a quadratic extension of F. Prove that the (monic) minimal polynomial is of the type described in the previous problem. Here we are assuming that char.F is $\neq 2$.

3.11. Take $F = \mathbb{Q}$ in the previous problem. Assume that $f \in \mathbb{Z}[X]$. Prove that we may choose P, Q, c satisfying
(i) c is a square-free integer, and
(ii) the coefficients of P and Q lie in $R = \{\frac{m}{2^n} : m \geq 0, n \in \mathbb{Z}\}$.

Deduce that if p is an odd prime, then f modulo p, i.e. its image $\overline{f} \in \mathbb{F}_p[X]$ does not have an irreducible factor of degree 3.
(this was an example I gave on Wednesday first week (without a proof) of a degree four extension of $\mathbb{Q}$ that does not contain a quadratic extension)
Hint for part (ii). If $Q(X) = X^2 + uX + v$, on examining the coefficient of X^3 in f, we see that $2u \in \mathbb{Z}$. Thus $u \in R$. Now $f \in \mathbb{Z}[X] \subset R[X]$. It follows that $f(X - \frac{u}{2}) \in R[X]$. We put $\widehat{f}(X) = f(X - \frac{u}{2}), \widehat{Q}(X) = Q(X - \frac{u}{2}), \widehat{P}(X) = P(X - \frac{u}{2})$. We observe $\widehat{f} = \widehat{Q}^2 - c\widehat{P}^2$. Note that $\widehat{Q}(X) = X^2 + \widehat{Q}(0)$.

Case 1: $\widehat{Q}(0) \in R$. It follows that $\widehat{Q} \in R[X]$. Also $c\widehat{P}^2 = \widehat{Q}^2 - \widehat{f} \in R[X]$. Because c is a square-free integer, it follows that $\widehat{P}^2 \in R[X]$. By examining the leading coefficient and constant coefficient of $\widehat{P}^2$, we see that $\widehat{P}$ itself belongs to $R[X]$. It follows that P, Q belong to $R[X]$, because $P(X) = \widehat{P}(X + \frac{u}{2})$ and $Q(X) = \widehat{Q}(X + \frac{u}{2})$.
Case 2: $\widehat{Q}(0) \notin R$. In which case, $\widehat{Q}(0) = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, and we have an odd prime p that does not divide a, but divides b. Let k be the highest power of p that divides b. Let $\widehat{P} = r_1 X + r_0$ and let v_1 and v_0 be the highest powers of p that divide the denominator of r_1 and r_0 (when expressed as reduced fractions).
The equation $\widehat{f}(0) = \widehat{Q}(0)^2 - c\widehat{P}(0)^2$ shows that p does not divide c, and also that $k = 2v_0$. (Here we are using once again the squarefree assumption on c).
Examining the degree two coefficient of f, we see that $k = v_1$.
Examining the degree one coefficient of f, we see that the highest power of p that divides it is $v_0 + v_1$, and that is impossible because $f \in R[X]$. Thus case 2 does not occur.

4

4.1. Let R be a commutative ring and let $T \in \mathrm{M}_n(R)$. Show that for every $v \in R^n$, there exists $w \in R^n$ such that $Tw = \det(T)v$.
Hint: This is a consequence of the definition of the adjoint matrix $\mathrm{adj}(T)$ and the fact that $T.\mathrm{adj}(T)$ equals the scalar matrix $\det(T)$.
Remark: In reality, the above adjoint matrix is simply $\Lambda^{n-1}(T)$. Therefore this problem could be stated and solved entirely within the framework of exterior algebras, with no reference to matrices.

4.2. With R, n, T as above, assume that R is an integral domain. Prove that $T : R^n \to R^n$ is one-to-one if and only if $\det(T)$ is nonzero.
Hint: Let K be the fraction field of R. We may regard T as a member of $\mathrm{M}_n(K)$.

4.3. Let R be a subring of a commutative ring S. Assume that S, when regarded as a R-module, is free of rank n. Prove that for every $\alpha \in S$, there exists $\beta \in S$ such that $\mathrm{Norm}_R^S(\alpha) = \beta\alpha$.
Show that if S is an integral domain, then $\mathrm{Norm}_R^S(\alpha) \neq 0$.

4.4. Let E be a field extension of F of degree n.
(i) Prove that $E[X]$, when regarded as a module over its subring $F[X]$, is free of rank n.
(ii) Let $0 \neq f \in E[X]$. Prove that there is some $g \in E[X]$ such that $gf = h$ wher $0 \neq h \in F[X]$.
Hint: Consider $h = \mathrm{Norm}_{F[X]}^{E[X]}(f)$.
(iii) Prove that $E(X)$ is a field extension of $F(X)$ of degree n. More precisely, show that if $w_1, ..., w_n$ is a F-basis for E, then $w_1, ..., w_n$ is also a $F(X)$-basis for $E(X)$.

4.5. With E and F as in the previous problem, show that $E(X_1, ..., X_d)$ is a field extension of $F(X_1, ..., X_d)$ of degree n.

4.6. Let F be any field. We have an action of the permutation group S_d on the polynomial ring $F[X_1, X_2, ..., X_d]$ by permuting the variables: for $\sigma \in S_d$, we define $\sigma f(X_1, ..., X_n) = f(X_{\sigma(1)}, ..., X_{\sigma(n)})$. This action of S_d on $F[X_1, ..., X_d]$ extends uniquely to an action of S_d on its fraction field $F(X_1, ..., X_n)$.

Employ Emil Artin's theorem to deduce that there is a finite Galois extension of fields with S_d as Galois group.

4.7. Show that every finite group can be realised as the Galois group of some finite Galois extension of fields.

4.8. Let $q = p^k$ where p is a prime. Let E be a finite field extension of $\mathbb{F}_q$ of degree n. Prove that E is a Galois extension of $\mathbb{F}_q$. Define $\sigma(x) = x^q$ for all $x \in E$. Prove that σ belongs to $\mathrm{Gal}(E/\mathbb{F}_q)$, and in fact generates this group.

4.9. Given an automorphism σ of a ring R, denote by R^σ the subring $\{a \in R : a = \sigma a\}$.

Let F be a field of characteristic zero. Define $\sigma f(X) = f(X + 1)$ for all $f \in F[X]$. Note that σ also gives rise to an automorphism of its fraction field $F(X)$. Prove that $F = F[X]^\sigma = F(X)^\sigma$

4.10. Let F be a field of characteristic $p > 0$. With σ as in the previous problem, show that $F(X)$ is a Galois extension of $F(X)^\sigma$ of degree p.

Do you know what $F[X]^\sigma$ and $F(X)^\sigma$ are?

5

5.1. Let L be a finite Galois extension of F. Let H_1 and H_2 be subgroups of $G = \mathrm{Gal}(L/F)$ and consider their fixed fields $E_1 = L^{H_1}$ and $E_2 = L^{H_2}$ respectively. Prove that $\mathrm{Gal}(L/E_1E_2)$ equals $H_1 \cap H_2$.

5.2. With notation as in the previous problem, show that $\mathrm{Gal}(L/E_1 \cap E_2)$ is the subgroup of G generated by H_1 and H_2.

5.3. Given $F \subset E \subset E'$ and $F \subset K \subset E'$, where F, E, K are subfields of E'.
It is not assumed that E is an algebraic extension of F Prove that

(1) If K is a finite separable extension of F, then EK is a finite separable extension of E.
(2) If K is a finite normal extension of F, then EK is a finite normal extension of E.
(3) If K is a finite Galois extension of F, then EK is a finite Galois extension of E.

5.4. Assuming the hypothesis of part (3) of the previous problem, show that $\sigma \mapsto \sigma|_K$ gives an isomorphism $\mathrm{Gal}(EK/E) \to \mathrm{Gal}(K/K \cap E)$.
Warning If your proof never relies on the Fundamental Thm of Galois theory, it is likely to be wrong. So, state precisely where you appeal to this thm.

5.5. Let p be a prime, let n be a natural number, and let F be a field that contains a primitive p^n-th root of unity. Let $a \in F$. Show that if $\deg F(a^{1/p})/F) > 1$, then $\deg F(a^{1/p^n})/F) = p^n$.
Hint: let $E = F(b)$ where $b^{p^n} = a$. Is E a Galois extension of F?

Let $u = p^{n-1}$ and let $c = b^u$. Does a F-automorphism σ of $F(c)$ extend to an F-automorphism of $F(b)$?

The next two problems are the analogues of problems 2.1 and 2.2.

5.6. Assume that F contains p distinct p-th roots of unity, where p is a prime.
Let $a \in F^\times$ and let $E = F(a^{1/p})$. Show that the kernel of the natural homomorphism $F^\times/(F^\times)^p \to E^\times/(E^\times)^p$ is the cyclic subgroup generated by the image of a in $F^\times/(F^\times)^p$.

5.7. With the assumptions on p and F as in the previous problem, let $a_1, ..., a_r \in F^\times$.
(i)Show that $\deg F(a_1^{1/p}, a_2^{1/p}, ..., a_r^{1/p})/F) = p^s$ where $0 \leq s \leq r$.
(ii)Show that the order of the subgroup of $F^\times/(F^\times)^p$ generated by the images of $a_1, a_2, ..., a_r$ is p^s.

5.8. Let K/F be a finite Galois extension with Galois group G. Assume that K contains a primitive p-th root of unity. Let $a \in K^\times$. Prove that every normal extension of F that contains $K(a^{1/p})$ necessarily contains the field L obtained from K by adjoining p-th roots of $\sigma(a)$ for all $\sigma \in G$).

5.9. If in the previous problem, (i) $\mathrm{Gal}(L/F)$ is Abelian, and (ii) F contains a primitive p-th root of unity,
show that $a^{-1}\sigma(a) \in (K^\times)^p$ for every $\sigma \in \mathrm{Gal}(K/F)$.

5.10. In the previous problem, assume furthermore that p does not divide the order of $\mathrm{Gal}(K/F)$. Show hat there is some $b \in F$ such that $L = K(b^{1/p})$

5.11. Let F be a field which contains a primitive p-th root of unity ζ. Show that a cyclic extension K/F of degree p is contained in a cyclic extension of degree p^2 if and only if there exists $u \in K$ such that $\mathrm{Norm}_F^K(u) = \zeta$.
Hint: For $p = 2$, this was proved in class using Hilbert's Thm.90. That proof can be mimicked, relying on 5.9.

6

6.1. Let $f : A \to B$ and $g : B \to C$ be ring homomorphisms. Let $\beta_1, ..., \beta_m \in B$ and let $\gamma_1, ..., \gamma_n \in C$.

(1) Assume that B, when regarded as a left A-module, is generated by $\beta_1, ..., \beta_m$, and also that C, when regarded as a left B-module, is generated by $\gamma_1, ..., \gamma_n \in C$.
Show that C, when regarded as a A-module, is generated by $\gamma_i.g(\beta_j)$ for all $1 \leq i \leq n, 1 \leq j \leq m$.

(2) Assume now that B is a free A-module with the β_i as basis, and C is a free B-module with the γ_j as basis. Show that C is A-free with the given generators in part (1) as basis.

6.2. Let $f(T) = T^n - a_1T^{n-1} + ... + (-1)^n a_n \in A[T]$. Let $B = A[X_1, X_2, ..., X_n]/(s_1 - a_1, s_2 - a_2, ..., s_n - a_n)$, where $s_1, s_2, ..., s_n$ are the elementary symmetric polynomials in $X_1, X_2, ..., X_n$. Prove that B is a free A-module with basis (as the image in B) of the monomials $X_1^{m_1}X_2^{m_2}...X_n^{m_n}$ where all the m_i are non-negative integers such that $m_i + i \leq n$ for all $i = 1, 2, ..., n$.
Prove this for $n = 3$

In all the remaining problems of this section, F is a field of characteristic $p > 0$

6.3. Let F be a field of characteristic $p > 0$. Let A be a finite additive subgroup of F.
Let $f_A \in F[X]$ be the product of $(X - a)$, taken over all $a \in A$.
(i) Prove that $f_A(X + a) = f_A(X)$ for all $a \in A$.
(ii) Deduce that $f_A(X + Y) = f_A(X) + f_A(Y) \in F[X, Y]$.
Hint: Let $C = F[Y]$ and let $h(X) = -f_A(X + Y) + f_A(X) + f_A(Y) \in C[X]$. Use (i) to find more $c \in C$ such that $h(c) = 0$ than the degree of $h \in C[X]$.

6.4. Let $f \in F[X]$. Prove that $f(X + Y) = f(X) + f(Y)$ if and only if $f = a_0X + a_1X^p + ... + a_nX^{p^n}$ for some $n \geq 0$ and $a_0, ..., a_n \in F$.

6.5. Assume that F is algebraically closed. Show that $A \mapsto f_A$ is a one-to-one correspondence from the collection of additive subgroups $A \subset F$ of order p^n and the set of polynomials in $F[X]$ of the form $f = a_0X + a_1X^p + ... + a_{n-1}X^{p^{n-1}} + X^{p^n}$ with $a_0 \neq 0$.

7

7.1. Let $G = \mathrm{Gal}(K/F)$. Assume that the order of $\mu_n(F)$ is n.
Let $\chi : G \to \mu_n(F)$ be a homomorphism. Show that $V^\chi = \{a \in K : \sigma(a) = \chi(\sigma).a \forall \sigma \in G\}$ is a one-dimensional F-vector space of K.
Hint: Let $b \in K$. Let $a \in K$ denote the sum of $\chi(\sigma)^{-1}\sigma(b)$, taken over all $\sigma \in G$.
Show that a belongs to V^χ.
Use Dedekind's "linear independence of characters" to show that there is some $b \in K$ such that the above a is nonzero.

8