

Section 6.1

1. We have $r_1 = 2, r_2 = 1, r_3 = 1$ so $t_1 = 1, t_2 = 0, t_3 = 1$. The algorithm terminates in one step after subtraction of $(X_1 + X_2 + X_3)(X_1X_2X_3)$. The given polynomial can be expressed as e_1e_3 .
2. We have $r_1 = 2, r_2 = 1, r_3 = 0$ so $t_1 = 1, t_2 = 1, t_3 = 0$. At step 1, subtract $(X_1 + X_2 + X_3)(X_1X_2 + X_1X_3 + X_2X_3)$. The result is $-3X_1X_2X_3 + 4X_1X_2X_3 = X_1X_2X_3$. By inspection (or by a second step of the algorithm), the given polynomial can be expressed as $e_1e_2 + e_3$.
3. Equation (1) follows upon taking $\sigma_1(h)$ outside the summation and using the linear dependence. Equation (2) is also a consequence of the linear dependence, because $\sigma_i(h)\sigma_i(g) = \sigma_i(hg)$.
4. By hypothesis, the characters are distinct, so for some $h \in G$ we have $\sigma_1(h) \neq \sigma_2(h)$. Thus in (3), each a_i is nonzero and

$$\sigma_1(h) - \sigma_i(h) \begin{cases} = 0 & \text{if } i = 1; \\ \neq 0 & \text{if } i = 2. \end{cases}$$

This contradicts the minimality of r . (Note that the $i = 2$ case is important, since there is no contradiction if $\sigma_1(h) - \sigma_i(h) = 0$ for all i .)

5. By (3.5.10), the Galois group consists of the identity alone. Since the identity fixes all elements, the fixed field of G is $\mathbb{Q}(\sqrt[3]{2})$.
6. Since $\mathbb{C} = \mathbb{R}[i]$, an \mathbb{R} -automorphism σ of \mathbb{C} is determined by its action on i . Since σ must permute the roots of $X^2 + 1$ by (3.5.1), we have $\sigma(i) = i$ or $-i$. Thus the Galois group has two elements, the identity automorphism and complex conjugation.
7. The complex number z is fixed by complex conjugation if and only if z is real, so the fixed field is \mathbb{R} .

Section 6.2

1. The right side is a subset of the left since both E_i and E_{i+1}^p are contained in E_{i+1} . Since E_i is contained in the set on the right, it is enough to show that $\alpha_{i+1} \in E_i(E_{i+1}^p)$. By hypothesis, α_{i+1} is separable over F , hence over $E_i(\alpha_{i+1}^p)$. By Section 3.4, Problem 3, $\alpha_{i+1} \in E_i(\alpha_{i+1}^p) \subseteq E_i(E_{i+1}^p)$.
2. Apply Section 3.4, Problem 7, with $E = F(E^p)$ replaced by $E_{i+1} = E_i(E_{i+1}^p)$, to conclude that E_{i+1} is separable over E_i . By the induction hypothesis, E_i is separable over F . By transitivity of separable extensions (Section 3.4, Problem 8), E_{i+1} is separable over F . By induction, E/F is separable.
3. Let f_i be the minimal polynomial of α_i over F . Then E is a splitting field for $f = f_1 \cdots f_n$ over F , and the result follows.
4. This is a corollary of part 2 of the fundamental theorem, with F replaced by K_{i-1} and G replaced by $\text{Gal}(E/K_{i-1}) = H_{i-1}$.
5. $E(A)$ is a field containing $E \geq F$ and A , hence $E(A)$ contains E and K , so that by definition of composite, $EK \leq E(A)$. But any field (in particular EK) that contains E and K contains E and A , hence contains $E(A)$. Thus $E(A) \leq EK$.
6. If $\sigma \in G$, define $\Psi(\sigma)(\tau(x)) = \tau\sigma(x)$, $x \in E$. Then $\psi(\sigma) \in G'$. [If $y = \tau(x) \in F'$ with $x \in F$, then $\Psi(\sigma)y = \Psi(\sigma)\tau x = \tau\sigma(x) = \tau(x) = y$.] Now $\Psi(\sigma_1\sigma_2\tau(x)) = \tau\sigma_1\sigma_2(x)$ and $\Psi(\sigma_1)\Psi(\sigma_2)\tau(x) = \Psi(\sigma_1)\tau\sigma_2(x) = \tau\sigma_1\sigma_2(x)$, so Ψ is a group homomorphism. The inverse of Ψ is given by $\Psi'(\sigma')\tau^{-1}y = \tau^{-1}\sigma'(y)$, $\sigma' \in G'$, $y \in E'$. To see this, we compute

$$\Psi'(\Psi(\sigma))\tau^{-1}y = \tau^{-1}\Psi(\sigma)y = \tau^{-1}\Psi(\sigma)\tau x = \tau^{-1}\tau\sigma(x) = \sigma(x) = \sigma(\tau^{-1}y).$$

Thus $\Psi'\Psi$ is the identity on G .

7. Since H' is a normal subgroup of G , its fixed field $L = \mathcal{F}(H')$ is normal over F , so by minimality of the normal closure, we have $N \subseteq L$. But all fixed fields are subfields of N , so

$L \subseteq N$, and consequently $L = N$.

8. If $\sigma \in H'$, then σ fixes everything in the fixed field N , so σ is the identity. Thus the largest normal subgroup of G that is contained in H is trivial. But this largest normal subgroup is the core of H in G , and the resulting formula follows from Problems 4 and 5 of Section 5.1.

Section 6.3

- $G = \{\sigma_1, \dots, \sigma_n\}$ where σ_i is the unique F -automorphism of E that takes α to α_i .
- We must find an α such that $1, \alpha, \dots, \alpha^{n-1}$ is a basis for E/\mathbb{Q} . If $\alpha = b_1x_1 + \dots + b_nx_n$, we can compute the various powers of α and write $\alpha^i = c_{i1}x_1 + \dots + c_{in}x_n$, $i = 0, 1, \dots, n-1$, where each c_{ij} is a rational number. The powers of α will form a basis iff $\det[c_{ij}] \neq 0$. This will happen “with probability 1”; if a particular choice of the b_i yields $\det[c_{ij}] = 0$, a slight perturbation of the b_i will produce a nonzero determinant.
- By (6.3.1), we may regard G as a group of permutations of the roots $\alpha_1, \dots, \alpha_n$ of f , and therefore G is isomorphic to a subgroup H of S_n . Since G acts transitively on the α_i (see (6.3.1)), the natural action of H on $\{1, 2, \dots, n\}$ is transitive. [For an earlier appearance of the natural action, see the discussion before (5.3.1).]
- The Galois group G must be isomorphic to a transitive subgroup of S_2 , which is cyclic of order 2. There is only one transitive subgroup of S_2 , namely S_2 itself, so G is a cyclic group of order 2.
- Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, the Galois group G has order 4. [Note that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ because $a + b\sqrt{2}$ can never be $\sqrt{3}$ for $a, b \in \mathbb{Q}$.] An automorphism σ in G must take $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$. Thus σ is either the identity or has order 2. Now a group in which every element has order 1 or 2 must be abelian, regardless of the size of the group [($ab)(ab) = 1$, so $ab = b^{-1}a^{-1} = ba$]. Since G is not cyclic, it must be isomorphic to the four group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. (See the analysis in (4.6.4).)
- Let H be the subgroup generated by H_1 and H_2 , that is, by $H_1 \cup H_2$. If $\sigma \in H_1 \cup H_2$, then σ fixes $K_1 \cap K_2 = K$. Since H consists of all finite products (= compositions) of elements in H_1 or H_2 , everything in H fixes K , so that $K \subseteq \mathcal{F}(H)$. On the other hand, if $x \in \mathcal{F}(H)$ but $x \notin K$, say $x \notin K_1$. Then some $\tau \in H_1 \subseteq H$ fails to fix x , so $x \notin \mathcal{F}(H)$, a contradiction. Therefore $K = \mathcal{F}(H)$.
- The fixed field is K_1K_2 , the composite of K_1 and K_2 . For if σ fixes K_1K_2 , then it fixes both K_1 and K_2 , so σ belongs to $H_1 \cap H_2$. Conversely, if $\sigma \in H_1 \cap H_2$, then σ is the identity on both K_1 and K_2 . But by the explicit form of K_1K_2 (see Section 3.1, Problem 1 and Section 6.2, Problem 5), σ is the identity on K_1K_2 . Thus $\mathcal{F}(H_1 \cap H_2) = K_1K_2$.
- We have $E = F(\alpha_1, \dots, \alpha_n)$, where the α_i are the roots of f . Since $\min(\alpha_i, F)$ divides the separable polynomial f , each α_i is separable over F . By Section 6.2, Problem 1, E is separable over F .
- Since $[\mathbb{Q}(\theta, i)/\mathbb{Q}] = [\mathbb{Q}(\theta)/\mathbb{Q}][\mathbb{Q}(\theta, i)/\mathbb{Q}(\theta)] = 4 \times 2 = 8$, we have $|G| = 8$. Any $\sigma \in G$ must map θ to a root of f (4 choices), and i to a root of $X^2 + 1$ (2 choices, i or $-i$). Since σ is determined by its action on θ and i , we have found all 8 members of G .
- Let $\sigma(\theta) = i\theta$, $\sigma(i) = i$, and let $\tau(\theta) = \theta$, $\tau(i) = -i$. Then $\sigma^4 = 1$, $\tau^2 = 1$, and the automorphisms $1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$ are distinct (by direct verification). Also, we have $\sigma\tau = \tau\sigma^{-1} = \tau\sigma^3$. The result follows from the analysis of the dihedral group in Section 5.8.
- By direct verification, every member of N fixes $i\theta^2 = i\sqrt{2}$. Since N has index 2 in G , the fixed field of N has degree 2 over \mathbb{Q} . But the minimal polynomial of $i\sqrt{2}$ over \mathbb{Q} is $X^2 + 2$, and it follows that $\mathcal{F}(N) = \mathbb{Q}(i\sqrt{2})$. $\mathcal{F}(N)$ is the splitting field of $X^2 + 2$ over \mathbb{Q} and is therefore normal over \mathbb{Q} , as predicted by Galois theory.

Section 6.4

- We have $\alpha^4 = 1 + \alpha + \alpha^2 + \alpha^3$ and $\alpha^5 = 1$. Thus the powers of α do not exhaust the nonzero elements of $GF(16)$.
- We may assume that $E = GF(p^n)$ and that E contains $F = GF(p^m)$, where $n = md$. Then $[E : F] = [E : \mathbb{F}_p]/[F : \mathbb{F}_p] = n/m = d$. Since E/F is separable, we have $E = F(\alpha)$ by

the theorem of the primitive element. The minimal polynomial of α over F is an irreducible polynomial of degree d .

3. Exactly as in (6.4.5), carry out a long division of $X^n - 1$ by $X^m - 1$. The division will be successful iff m divides n .

4. Since the b_i belong to L , we have $K \subseteq L$, and since $h \in L[X]$, it follows that $g|h$. But $g \in K[X]$ by definition of K , so $h|g$. Since g and h are monic, they must be equal. In particular, they have the same degree, so $[E : L] = [E : K]$. Since $K \subseteq L$, we have $L = K$.

5. Since $L = K$, L is completely determined by g . But if $f = \min(\alpha, F)$, then g divides f . Since f has only finitely many irreducible divisors, there can only be finitely many intermediate fields L .

6. Since there are finitely many intermediate fields between E and F , the same is true between L and F . By induction hypothesis, $L = F(\beta)$ for some $\beta \in L$. Thus $E = L(\alpha_n) = F(\beta, \alpha_n)$.

7. By hypothesis, there are only finitely many fields of the form $F(c\beta + \alpha_n)$, $c \in F$. But there are infinitely many choices of c , and the result follows.

8. Since $E = F(\beta, \alpha_n)$, it suffices to show that $\beta \in F(c\beta + \alpha_n)$. This holds because

$$\beta = \frac{(c\beta + \alpha_n) - (d\beta + \alpha_n)}{c - d}.$$

9. Let $\sigma : F \rightarrow F$ be the Frobenius automorphism, given by $\sigma(x) = x^p$. Let $f = \min(\alpha, \mathbb{F}_p)$ and $g = \min(\alpha^p, \mathbb{F}_p)$. Then $f(\alpha^p) = f(\sigma(\alpha)) = \sigma(f(\alpha))$ since σ is a monomorphism, and $\sigma(f(\alpha)) = \sigma(0) = 0$. Thus g divides the monic irreducible polynomial f , so $g = f$.

10. By Problem 9, the subsets are $\{0\}$, $\{1, 3, 9\}$, $\{2, 6, 5\}$, $\{4, 12, 10\}$, and $\{7, 8, 11\}$. [For example, starting with 2, we have $2 \times 3 = 6, 6 \times 3 = 18 \equiv 5 \pmod{13}, 5 \times 3 = 15 \equiv 2 \pmod{13}$.] In the second case, we get

$$\{0\}, \{1, 2, 4, 8\}, \{3, 6, 9, 12\}, \{5, 10\}, \{7, 14, 13, 11\}.$$

Section 6.5

1. $\Psi_n(X^p) = \prod_i (X^p - \omega_i)$ where the ω_i are the primitive n^{th} roots of unity. But the roots of $X^p - \omega_i$ are the p^{th} roots of ω_i , which must be primitive np^{th} roots of unity because p is prime and p divides n . The result follows. (The map $\theta \rightarrow \theta^p$ is a bijection between primitive np^{th} roots of unity and primitive n^{th} roots of unity, because $\varphi(np) = \varphi(n)$.)

2. By (6.5.1) and (6.5.6), the Galois group of the n^{th} cyclotomic extension of \mathbb{Q} can be identified with the group of automorphisms of the cyclic group of n^{th} roots of unity. By (6.5.6), the Galois group is isomorphic to U_n , and the result follows.

3. The powers of 3 mod 7 are 3, $9 \equiv 2$, 6, $18 \equiv 4$, $12 \equiv 5$, 1.

4. This follows from Problem 3 and (1.1.4).

5. $\sigma_6(\omega + \omega^6) = \omega^6 + \omega^{36} = \omega + \omega^6$, so $\omega + \omega^6 \in K$. Now $\omega + \omega^6 = \omega + \omega^{-1} = 2 \cos 2\pi/7$, so ω satisfies a quadratic equation over $\mathbb{Q}(\cos 2\pi/7)$. By (3.1.9),

$$[\mathbb{Q}_7 : \mathbb{Q}] = [\mathbb{Q}_7 : K][K : \mathbb{Q}(\cos 2\pi/7)][\mathbb{Q}(\cos 2\pi/7) : \mathbb{Q}]$$

where the term on the left is 6, the first term on the right is $|\langle \sigma_6 \rangle| = 2$, and the second term on the right is (by the above remarks) 1 or 2. But $[K : \mathbb{Q}(\cos 2\pi/7)]$ cannot be 2 (since 6 is not a multiple of 4), so we must have $K = \mathbb{Q}(\cos 2\pi/7)$.

6. $\sigma_2(\omega + \omega^2 + \omega^4) = \omega^2 + \omega^4 + \omega^8 = \omega + \omega^2 + \omega^4$, so $\omega + \omega^2 + \omega^4 \in L$; $\sigma_3(\omega + \omega^2 + \omega^4) = \omega^3 + \omega^6 + \omega^{12} = \omega^3 + \omega^5 + \omega^6 \neq \omega + \omega^2 + \omega^4$, so $\omega + \omega^2 + \omega^4 \notin \mathbb{Q}$. [If $\omega^3 + \omega^5 + \omega^6 = \omega + \omega^2 + \omega^4$, then we have two distinct monic polynomials of degree 6 satisfied by ω (the other is $\Psi_7(X)$), which is impossible.]

7. By the fundamental theorem, $[L : \mathbb{Q}] = [G : \langle \sigma_2 \rangle] = 2$, so we must have $L =$

$\mathbb{Q}(\omega + \omega^2 + \omega^4)$.

8. The roots of Ψ_q are the p^r th roots of unity that are not p^{r-1} th roots of unity. Thus

$$\Psi_q(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = \frac{t^p - 1}{t - 1}$$

and the result follows.

9. By Problem 1,

$$\Psi_{18}(X) = \Psi_{(3)(6)}(X) = \Psi_6(X^3) = X^6 - X^3 + 1.$$

Section 6.6

1. f is irreducible by Eisenstein, and the Galois group is S_3 . This follows from (6.6.7) or via the discriminant criterion of (6.6.3); we have $D(f) = -27(4) = -108$, which is not a square in \mathbb{Q} .

2. f is irreducible by the rational root test, and $D(f) = -4(-3)^3 - 27 = 108 - 27 = 81$, a square in \mathbb{Q} . Thus the Galois group is A_3 .

3. f is irreducible by Eisenstein. The derivative is $f'(X) = 5X^4 - 40X^3 = 5X^3(X - 8)$. We have $f'(x)$ positive for $x < 0$ and for $x > 8$, and $f'(x)$ negative for $0 < x < 8$. Since $f(0) > 0$ and $f(8) < 0$, graphing techniques from calculus show that f has exactly 3 real roots. By (6.6.7), $G = S_3$.

4. f is irreducible by the rational root test. By the formula for the discriminant of a general cubic with $a = 3, b = -2, c = 1$, we have $D = 9(-8) - 4(-8) - 27 - 18(6) = -175$. Alternatively, if we replace X by $X - \frac{a}{3} = X - 1$, the resulting polynomial is $g(X) = X^3 - 5X + 5$, whose discriminant is $-4(-5)^3 - 27(25) = -175$. In any event, D is not a square in \mathbb{Q} , so $G = S_3$. (Notice also that g is irreducible by Eisenstein, so we could have avoided the rational root test at the beginning.)

5. If f is reducible, then it is the product of a linear factor and a quadratic polynomial g . If g is irreducible, then G is cyclic of order 2 (section 6.3, Problem 4). If g is reducible, then all roots of f are in the base field, and G is trivial.

6. Let the roots be $a, b + ic$ and $b - ic$. Then

$$\Delta = (a - b - ic)(a - b + ic)2ic = ((a - b)^2 + c^2)2ic$$

and since $i^2 = -1$, we have $D < 0$. Since D cannot be a square in \mathbb{Q} , the Galois group is S_3 . [This also follows from (6.6.7).]

7. If the roots are a, b and c , then $D = (a - b)^2(a - c)^2(b - c)^2 > 0$. The result follows from (6.6.3).

Section 6.7

1. By (6.7.2), the Galois group of $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ is \mathbb{Z}_2 for $m = 2, 3, 5, 7$. It follows that the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})/\mathbb{Q}$ is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. See (6.7.5), and note that \mathbb{Q} contains a primitive square root of unity, namely -1. (It is not so easy to prove that the Galois group has order 16. One approach is via the technique of Section 7.3, Problems 9 and 10.)

2. Yes. Let E be the p^{th} cyclotomic extension of \mathbb{Q} , where p is prime. If $p > 2$, then \mathbb{Q} does not contain a primitive p^{th} root of unity. By (6.5.6), the Galois group is isomorphic to the group of units mod p , which is cyclic.

3. Since the derivative of $f(X) = X^n - a$ is $nX^{n-1} \neq 0$, it follows from (3.4.2) that f has n distinct roots β_1, \dots, β_n in E . Since $\beta_i^n = a$ and $\beta_i^{-n} = a^{-1}$, there are n distinct n^{th} roots of unity in E , namely $1 = \beta_1\beta_1^{-1}, \beta_2\beta_1^{-1}, \dots, \beta_n\beta_1^{-1}$. Since the group of n^{th} roots of unity is cyclic, there must be a primitive n^{th} root of unity in E .

4. Each root of g is of the form $\omega^i\theta$, so $g_0 = \omega^k\theta^d$ for some k . Since $\omega^p = 1$, we have

$g_0^p = \theta^{dp}$. But $c = \theta^p$ since θ is also a root of f , and the result follows.

5. By Problem 4 we have

$$c = c^1 = c^{ad}c^{bp} = g_0^{ap}c^{bp} = (g_0^a c^b)^p$$

with $g_0^a c^b \in F$. Thus $g_0^a c^b$ is a root of f in F .

6. $[E : F(\omega)]$ divides p and is less than p by (6.7.2); note that E is also a splitting field for f over $F(\omega)$. Thus $[E : F(\omega)]$ must be 1, so $E = F(\omega)$.

7. F contains a primitive p^{th} root of unity ω iff $E(= F(\omega)) = F$ iff $X^p - c$ splits over F .

8. By induction, $\sigma^j(\theta) = \theta + j$, $0 \leq j \leq p-1$. Thus the subgroup of G that fixes θ , hence fixes $F(\theta)$, consists only of the identity. By the fundamental theorem, $E = F(\theta)$.

9. We have $\sigma(\theta^p - \theta) = \sigma(\theta)^p - \sigma(\theta) = (\theta+1)^p - (\theta+1) = \theta^p - \theta$ in characteristic p . Thus $\theta^p - \theta$ belongs to the fixed field of G , which is F . Let $a = \theta^p - \theta$, and the result follows.

10. Since $f(\theta) = 0$, $\min(\theta, F)$ divides f . But the degree of the minimal polynomial is $[F(\theta) : F] = [E : F] = p = \deg f$. Thus $f = \min(\theta, F)$, which is irreducible.

11. Since $\theta^p - \theta = a$, we have $(\theta+1)^p - (\theta+1) = \theta^p - \theta = a$. Inductively, $\theta, \theta+1, \dots, \theta+p-1$ are distinct roots of f in E , and since f has degree p , we have found all the roots and f is separable. Since E is a splitting field for f over F , we have $E = F(\theta)$.

12. By Problem 11, every root of f generates the same extension of F , namely E . But any monic irreducible factor of f is the minimal polynomial of at least one of the roots of f , and the result follows.

13. $[E : F] = [F(\theta) : F] = \deg(\min(\theta, F)) = \deg f = p$. Thus the Galois group has prime order p and is therefore cyclic.

Section 6.8

1. Take the real part of each term of the identity to get

$$\cos 3\theta = \cos^3 \theta + 3 \cos \theta (i \sin \theta)^2 = \cos^3 \theta - 3 \cos \theta (1 - \cos^2 \theta);$$

thus $\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta$. If $3\theta = \pi/3$, we have

$$\cos \pi/3 = 1/2 = 4\alpha^3 - 3\alpha$$

so $8\alpha^3 - 6\alpha - 1 = 0$. But $8X^3 - 6X - 1$ is irreducible over \mathbb{Q} (rational root test), so α is algebraic over \mathbb{Q} and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ (not a power of 2), a contradiction.

2. $X^3 - 2$ is irreducible by Eisenstein, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $\sqrt[3]{2}$ is not constructible.

3. The side of such a square would be $\sqrt{\pi}$, so $\sqrt{\pi}$, hence π , would be algebraic over \mathbb{Q} , a contradiction.

4. ω is a root of $X^2 - 2(\cos 2\pi/n)X + 1$ since $\cos 2\pi/n = \frac{1}{2}(\omega + \omega^{-1})$ and $\omega^2 - (\omega + \omega^{-1})\omega + 1 = 0$.

5. By (6.5.2), (6.5.5) and (3.1.9),

$$\varphi(n) = [\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}(\cos 2\pi/n)][\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}].$$

By Problem 4, $[\mathbb{Q}(\omega) : \mathbb{Q}(\cos 2\pi/n)] = 2$, and if the regular n -gon is constructible, then $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}]$ is a power of 2. The result follows.

6. By hypothesis, $G = \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is a 2-group since its order is $\varphi(n)$. Therefore every quotient group of G , in particular $\text{Gal}(\mathbb{Q}(\cos 2\pi/n)/\mathbb{Q})$, is a 2-group. [Note that by (6.5.1), G is abelian, hence every subgroup of G is normal, and therefore every intermediate field is a Galois extension of \mathbb{Q} . Thus part 2c of the fundamental theorem (6.2.1) applies.]

7. By the fundamental theorem (specifically, by Section 6.2, Problem 4), there are fields $\mathbb{Q} = K_0 \leq K_1 \leq \dots \leq K_r = \mathbb{Q}(\cos 2\pi/n)$ with $[K_i : K_{i-1}] = 2$ for all $i = 1, \dots, r$. Thus $\cos 2\pi/n$ is constructible.

8. If $n = p_1^{e_1} \cdots p_r^{e_r}$, then (see Section 1.1, Problem 13)

$$\varphi(n) = p_1^{e_1-1}(p_1 - 1) \cdots p_r^{e_r-1}(p_r - 1).$$

If $p_i \neq 2$, we must have $e_i = 1$, and in addition, $p_i - 1$ must be a power of 2. The result follows.

9. If m is not a power of 2, then m can be factored as ab where a is odd and $1 < b < m$. In the quotient $(X^a + 1)/(X + 1)$, set $X = 2^b$. It follows that $(2^m + 1)/(2^b + 1)$ is an integer. Since $1 < 2^b + 1 < 2^m + 1$, $2^m + 1$ cannot be prime.

10. Any permutation of the α_i induces an automorphism of E which fixes each e_i , hence fixes F . Thus the Galois group of f consists of all permutations of n letters.

11. Since S_n is not solvable, the general equation of degree n is not solvable by radicals if $n \geq 5$. In other words, if $n \geq 5$, there is no sequence of operations on e_1, \dots, e_n involving addition, subtraction, multiplication, division and extraction of m^{th} roots, that will yield the roots of f .

Section 6.9

1. If S is not maximal, keep adding elements to S until a maximal algebraically independent set is obtained. If we go all the way to T , then T is algebraically independent and spans E algebraically, hence is a transcendence basis. (Transfinite induction supplies the formal details.)

2. For the first statement, take $T = E$ in Problem 1. For the second statement, take $S = \emptyset$.

3. (i) implies (ii): Suppose that t_i satisfies $f(t_i) = b_0 + b_1 t_i + \dots + b_m t_i^m = 0$, with $b_j \in F(T \setminus \{t_i\})$. By forming a common denominator for the b_j , we may assume that the b_j are polynomials in $F[T \setminus \{t_i\}] \subseteq F[T]$. By (i), $b_j = 0$ for all j , so $f = 0$.

(ii) implies (iii): Note that $F(t_1, \dots, t_{i-1}) \subseteq F(T \setminus \{t_i\})$.

(iii) implies (i): Suppose that f is a nonzero polynomial in $F[X_1, \dots, X_m]$ such that $f(t_1, \dots, t_m) = 0$, where m is as small as possible. Then $f = h_0 + h_1 X_m + \dots + h_r X_m^r$ where the h_j belong to $F[X_1, \dots, X_{m-1}]$. Now $f(t_1, \dots, t_m) = b_0 + b_1 t_m + \dots + b_r t_m^r$ where $b_j = h_j(t_1, \dots, t_{m-1})$. If the b_j are not all zero, then t_m is algebraic over $F(t_1, \dots, t_{m-1})$, contradicting (iii). Thus $b_j \equiv 0$, so by minimality of m , $h_j \equiv 0$, so $f = 0$.

4. If $S \cup \{t\}$ is algebraically dependent over F , then there is a positive integer n and a nonzero polynomial f in $F[X_1, \dots, X_n, Z]$ such that $f(t_1, \dots, t_n, t) = 0$ for some $t_1, \dots, t_n \in S$. Since S is algebraically independent over F , f must involve Z . We may write $f = b_0 + b_1 Z + \dots + b_m Z^m$ where $b_m \neq 0$ and the b_j are polynomials in $F[X_1, \dots, X_n]$. But then t is algebraic over $F(S)$.

Conversely, if t is algebraic over $F(S)$, then for some positive integer n , there are elements $t_1, \dots, t_n \in S$ such that t is algebraic over $F(t_1, \dots, t_n)$. By Problem 3, $\{t_1, \dots, t_n, t\}$ is algebraically dependent over F , hence so is $S \cup \{t\}$.

5. Let $A = \{s_1, \dots, s_m, t_1, \dots, t_n\}$ be an arbitrary finite subset of $S \cup T$, with $s_i \in S$ and $t_j \in T$. By Problem 3, s_i is transcendental over $F(s_1, \dots, s_{i-1})$ and t_j is transcendental over $K(t_1, \dots, t_{j-1})$, hence over $F(s_1, \dots, s_m, t_1, \dots, t_{j-1})$ since $S \subseteq K$. Again by Problem 3, A is algebraically independent over F . Since A is arbitrary, $S \cup T$ is algebraically independent over F . Now if $t \in K$ then $\{t\}$ is algebraically dependent over K (t is a root of $X - t$). But if t also belongs to T , then T is algebraically dependent over K , contradicting the hypothesis. Thus K and T , hence S and T , are disjoint.

6. By Problem 5, $S \cup T$ is algebraically independent over F . By hypothesis, E is algebraic over $K(T)$ and K is algebraic over $F(S)$. Since each $t \in T$ is algebraic over $F(S)(T) = F(S \cup T)$, it follows that $K(T)$ is algebraic over $F(S \cup T)$. By (3.3.5), E is algebraic over $F(S \cup T)$. Therefore $S \cup T$ is a transcendence basis for E/F .

7. If T is algebraically independent over F , the map $f(X_1, \dots, X_n) \rightarrow f(t_1, \dots, t_n)$ extends to an F -isomorphism of $F(X_1, \dots, X_n)$ and $F(t_1, \dots, t_n)$. Conversely, assume that $F(T)$ is F -isomorphic to the rational function field. By Problem 2, there is a transcendence basis B for $F(T)/F$ such that $B \subseteq T$. By (6.9.7), the transcendence degree of $F(T)/F$ is $|T| = n$. By (6.9.5) or (6.9.6), $B = T$, so T is algebraically independent over F .

8. The “if” part is clear since $[K(z) : K]$ can’t be finite; if so, $[F : K] < \infty$. For the “only

if” part, z is algebraic over $K(x)$, so let

$$z^n + \varphi_{n-1}(x)z^{n-1} + \cdots + \varphi_0(x) = 0, \quad \varphi_i \in K(x).$$

Clear denominators to get a polynomial $f(z, x) = 0$, with coefficients of f in K . Now x must appear in f , otherwise z is not transcendental. Thus x is algebraic over $K(z)$, so $[K(z, x) : K(z)] < \infty$. Therefore

$$[F : K(z)] = [F : K(z, x)][K(z, x) : K(z)].$$

The first term on the right is finite since $K(x) \subseteq K(z, x)$, and the second term is finite, as we have just seen. Thus $[F : K(z)] < \infty$, and the result follows. ♣

9. We have $\text{tr deg}(\mathbb{C}/\mathbb{Q}) = c$, the cardinality of \mathbb{C} (or \mathbb{R}). For if \mathbb{C} has a countable transcendence basis z_1, z_2, \dots over \mathbb{Q} , then \mathbb{C} is algebraic over $\mathbb{Q}(z_1, z_2, \dots)$. Since a polynomial over \mathbb{Q} can be identified with a finite sequence of rationals, it follows that $|\mathbb{C}| = |\mathbb{Q}|$, a contradiction.

Section 7.1

1. Replace (iii) by (iv) and the proof goes through as before. If R is a field, then in (iii) implies (i), x is an eigenvalue of C , so $\det(xI - C) = 0$.
2. Replace (iii) by (v) and the proof goes through as before. [Since B is an $A[x]$ -module, in (iii) implies (i) we have $x\beta_i \in B$; when we obtain $[\det(xI - C)]b = 0$ for every $b \in B$, the hypothesis that B is faithful yields $\det(xI - C) = 0$.]
3. Multiply the equation by a^{n-1} to get

$$a^{-1} = -(c_{n-1} + \cdots + c_1 a^{n-2} + c_0 a^{n-1}) \in A.$$

4. Since $A[b]$ is a subring of B , it is an integral domain. Thus if $bz = 0$ and $b \neq 0$, then $z = 0$.
5. Any linear transformation on a finite-dimensional vector space is injective iff it is surjective. Thus if $b \in B$ and $b \neq 0$, there is an element $c \in A[b] \subseteq B$ such that $bc = 1$. Therefore B is a field.
6. P is the preimage of Q under the inclusion map of A into B , so P is a prime ideal. The map $a + P \rightarrow a + Q$ is a well-defined injection of A/P into B/Q , since $P = Q \cap A$. Thus A/P can be viewed as a subring of B/Q .
7. If $b + Q \in B/Q$, then b satisfies an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0, \quad a_i \in A.$$

By Problem 6, $b + Q$ satisfies the same equation with a_i replaced by $a_i + P$ for all i . Thus B/Q is integral over A/P .

8. By Problems 3-5, A/P is a field if and only if B/Q is a field, and the result follows. (Note that since Q is a prime ideal, B/Q is an integral domain, as required in the hypothesis of the result just quoted.)

Section 7.2

1. By the quadratic formula, $L = \mathbb{Q}(\sqrt{b^2 - 4c})$. Since $b^2 - 4c \in \mathbb{Q}$, we may write $b^2 - 4c = s/t = st/t^2$ for relatively prime integers s and t . We also have $s = uy^2$ and $t = vz^2$ where $u, v, y, z \in \mathbb{Z}$, with u and v relatively prime and square-free. Thus $L = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{d})$.
2. If $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{e})$, then $\sqrt{d} = a + b\sqrt{e}$ for rational numbers a and b . Thus $d = a^2 + b^2e + 2ab\sqrt{e}$, so \sqrt{e} is rational, a contradiction (unless $a = 0$ and $b = 1$).
3. Any isomorphism of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{e})$ must carry \sqrt{d} into $a + b\sqrt{e}$ for rational numbers a and b . Thus d is mapped to $a^2 + b^2e + 2ab\sqrt{e}$. But a \mathbb{Q} -isomorphism maps d to d , and we

reach a contradiction as in Problem 2.

4. Since $\omega_n = \omega_{2n}^2$ we have $\omega_n \in \mathbb{Q}(\omega_{2n})$, so $\mathbb{Q}(\omega_n) \subseteq \mathbb{Q}(\omega_{2n})$. If n is odd then $n + 1 = 2r$, so

$$\omega_{2n} = -\omega_{2n}^{2r} = -(\omega_{2n}^2)^r = -\omega_n^r.$$

Therefore $\mathbb{Q}(\omega_{2n}) \subseteq \mathbb{Q}(\omega_n)$.

5. Let f be a monic polynomial over \mathbb{Z} with $f(x) = 0$. If f is factorable over \mathbb{Q} , then it is factorable over \mathbb{Z} by (2.9.2). Thus $\min(x, \mathbb{Q})$ is the monic polynomial in $\mathbb{Z}[X]$ of least degree such that $f(x) = 0$.

6. $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ where $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ is a primitive cube root of unity.

7. If $n = [L : \mathbb{Q}]$, then an integral basis consists of n elements of L that are linearly independent over \mathbb{Z} , hence over \mathbb{Q} . (A linear dependence relation over \mathbb{Q} can be converted to one over \mathbb{Z} by multiplying by a common denominator.)

Section 7.2

1. By the quadratic formula, $L = \mathbb{Q}(\sqrt{b^2 - 4c})$. Since $b^2 - 4c \in \mathbb{Q}$, we may write $b^2 - 4c = s/t = st/t^2$ for relatively prime integers s and t . We also have $s = uy^2$ and $t = vz^2$ where $u, v, y, z \in \mathbb{Z}$, with u and v relatively prime and square-free. Thus $L = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{d})$.

2. If $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{e})$, then $\sqrt{d} = a + b\sqrt{e}$ for rational numbers a and b . Thus $d = a^2 + b^2e + 2ab\sqrt{e}$, so \sqrt{e} is rational, a contradiction (unless $a = 0$ and $b = 1$).

3. Any isomorphism of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{e})$ must carry \sqrt{d} into $a + b\sqrt{e}$ for rational numbers a and b . Thus d is mapped to $a^2 + b^2e + 2ab\sqrt{e}$. But a \mathbb{Q} -isomorphism maps d to d , and we reach a contradiction as in Problem 2.

4. Since $\omega_n = \omega_{2n}^2$ we have $\omega_n \in \mathbb{Q}(\omega_{2n})$, so $\mathbb{Q}(\omega_n) \subseteq \mathbb{Q}(\omega_{2n})$. If n is odd then $n + 1 = 2r$, so

$$\omega_{2n} = -\omega_{2n}^{2r} = -(\omega_{2n}^2)^r = -\omega_n^r.$$

Therefore $\mathbb{Q}(\omega_{2n}) \subseteq \mathbb{Q}(\omega_n)$.

5. Let f be a monic polynomial over \mathbb{Z} with $f(x) = 0$. If f is factorable over \mathbb{Q} , then it is factorable over \mathbb{Z} by (2.9.2). Thus $\min(x, \mathbb{Q})$ is the monic polynomial in $\mathbb{Z}[X]$ of least degree such that $f(x) = 0$.

6. $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ where $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ is a primitive cube root of unity.

7. If $n = [L : \mathbb{Q}]$, then an integral basis consists of n elements of L that are linearly independent over \mathbb{Z} , hence over \mathbb{Q} . (A linear dependence relation over \mathbb{Q} can be converted to one over \mathbb{Z} by multiplying by a common denominator.)

Section 7.4

1. If $l(y) = 0$, then $(x, y) = 0$ for all x . Since the bilinear form is nondegenerate, we must have $y = 0$.

2. Since V and V^* have the same dimension n , the map $y \rightarrow l(y)$ is surjective.

3. We have $(x_i, y_j) = l(y_j)(x_i) = f_j(x_i) = \delta_{ij}$. Since the $f_j = l(y_j)$ form a basis, so do the y_j .

4. Write $x_i = \sum_{k=1}^n a_{ik}y_k$, and take the inner product of both sides with x_j to conclude that $a_{ij} = (x_i, x_j)$.

5. The “if” part was done in the proof of (7.4.10). If $\det C = \pm 1$, then C^{-1} has coefficients in \mathbb{Z} by Cramer’s rule.

6. If $d \not\equiv 1 \pmod{4}$, then by (7.2.3), 1 and \sqrt{d} form an integral basis. Since the trace of $a + b\sqrt{d}$ is $2a$ (Section 7.3, Problem 1), the field discriminant is

$$D = \det \begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} = 4d.$$

If $d \equiv 1 \pmod{4}$, then 1 and $\frac{1}{2}(1 + \sqrt{d})$ form an integral basis, and

$$\left[\frac{1}{2}(1 + \sqrt{d})\right]^2 = \frac{1}{4} + \frac{d}{4} + \frac{1}{2}\sqrt{d}.$$

Thus

$$D = \det \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix} = d.$$

7. The first statement follows because multiplication of each element of a group G by a particular element $g \in G$ permutes the elements of G . The plus and minus signs are balanced in $P + N$ and PN , before and after permutation. We can work in a Galois extension of \mathbb{Q} containing L , and each automorphism in the Galois group restricts to one of the σ_i on L . Thus $P + N$ and PN belong to the fixed field of the Galois group, which is \mathbb{Q} .

8. Since the x_j are algebraic integers, so are the $\sigma_i(x_j)$, as in the proof of (7.3.10). By (7.1.5), P and N , hence $P + N$ and PN , are algebraic integers. By (7.1.7), \mathbb{Z} is integrally closed, so by Problem 7, $P + N$ and PN belong to \mathbb{Z} .

9. $D = (P - N)^2 = (P + N)^2 - 4PN \equiv (P + N)^2 \pmod{4}$. But any square is congruent to 0 or 1 mod 4, and the result follows.

10. We have $y_i = \sum_{j=1}^n a_{ij}x_j$ with $a_{ij} \in \mathbb{Z}$. By (7.4.3), $D(y) = (\det A)^2 D(x)$. Since $D(y)$ is square-free, $\det A = \pm 1$, so A has an inverse with entries in \mathbb{Z} . Thus $x = A^{-1}y$, as claimed.

11. Every algebraic integer is a \mathbb{Z} -linear combination of the x_i , hence of the y_i by Problem 10. Since the y_i form a basis for L over \mathbb{Q} , they are linearly independent and the result follows.

12. No. For example, let $L = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer with $d \not\equiv 1 \pmod{4}$. (See Problem 6). The field discriminant is $4d$, which is not square-free.

13. This follows from the proof of (7.4.7).

Section 7.5

1. $A_0 \subset A_1 \subset A_2 \subset \dots$

2. Let $a/p^n \in B$, where p does not divide a . There are integers r and s such that $ra + sp^n = 1$. Thus $ra/p^n = 1/p^n$ in \mathbb{Q}/\mathbb{Z} , and $A_n \subseteq B$. If there is no upper bound on n , then $1/p^n \in B$ for all n (note $1/p^n = p/p^{n+1} = p^2/p^{n+2}$, etc.), hence $B = A$. If there is a largest n , then for every $m > n$, $B \cap A_m \subseteq A_n$ by maximality of n . Therefore $B = A_n$.

3. Let x_1, x_2, \dots be a basis for V . Let M_r be the subspace spanned by x_1, \dots, x_r , and L_r the subspace spanned by the $x_j, j > r$. If V is n -dimensional, then $V = L_0 > L_1 > \dots > L_{n-1} > L_n = 0$ is a composition series since a one-dimensional subspace is a simple module. [$V = M_n > M_{n-1} > \dots > M_1 > 0$ is another composition series.] Thus V is Noetherian and Artinian. If V is infinite-dimensional, then $M_1 < M_2 < \dots$ violates the acc, and $L_0 > L_1 > L_2 > \dots$ violates the dcc. Thus V is neither Noetherian nor Artinian. [Note that if V has an uncountable basis, there is no problem; just take a countably infinite subset of it.]

4. $l(M)$ is finite iff M has a composition series iff M is Noetherian and Artinian iff N and M/N are Noetherian and Artinian iff $l(N)$ and $l(M/N)$ are finite.

5. By Problem 4, the result holds when $l(M) = \infty$, so assume $l(M)$, hence $l(N)$ and $l(M/N)$, finite. Let $0 < N_1 < \dots < N_r = N$ be a composition series for N , and let $N/N < (M_1 + N)/N < \dots < (M_s + N)/N = M/N$ be a composition series for M/N . Then

$$0 < N_1 < \dots < N_r < M_1 + N < \dots < M_s + N = M$$

is a composition series for M . (The factors in the second part of the series are simple by the third isomorphism theorem.) It follows that $l(M) = r + s = l(N) + l(M/N)$.

6. By (7.5.9), R is a Noetherian S -module, hence a Noetherian R -module. (Any R -submodule T of R is, in particular, an S -submodule of R . Therefore T is finitely generated.)

7. Yes. Map a polynomial to its constant term and apply the first isomorphism theorem to show that $R \cong R[X]/(X)$. Thus R is a quotient of a Noetherian R -module, so is Noetherian by (7.5.7).

8. If there is an infinite descending chain of submodules M_i of M , then the intersection $N = \bigcap_i M_i$ cannot be expressed as the intersection of finitely many M_i . By the correspondence theorem, $\bigcap_i (M_i/N) = 0$, but no finite intersection of the submodules M_i/N of M/N

is 0. Thus M/N is not finitely cogenerated. Conversely, suppose that M/N is not finitely cogenerated. By the correspondence theorem, we have $\bigcap_{\alpha} M_{\alpha} = N$, but no finite intersection of the M_{α} is N . Pick any M_{α} and call it M_1 . If $M_1 \subseteq M_{\alpha}$ for all α , then $M_1 = N$, a contradiction. Thus we can find $M_{\alpha} = M_2$ such that $M_1 \supset M_1 \cap M_2$. Continue inductively to produce an infinite descending chain.

Section 7.6

1. The “only if” part follows from (7.6.2). If the given condition is satisfied and $ab \in P$, then $(a)(b) \subseteq P$, hence $(a) \subseteq P$ or $(b) \subseteq P$, and the result follows.
2. If $x_i \notin P_i$ for some i , then $x_i \in I \setminus \bigcup_{j=1}^n P_j$ and we are finished.
3. Since I is an ideal, $x \in I$. Say $x \in P_1$. All terms in the sum that involve x_1 belong to P_1 by Problem 2. The remaining term $x_2 \cdots x_n$ is the difference of two elements in P_1 , hence $x_2 \cdots x_n \in P_1$. Since P_1 is prime, $x_j \in P_1$ for some $j \neq 1$, contradicting the choice of x_j .
4. The product of ideals is always contained in the intersection. If I and J are relatively prime, then $1 = x + y$ with $x \in I$ and $y \in J$. If $z \in I \cap J$, then $z = z1 = zx + zy \in IJ$. The general result follows by induction, along with the computation

$$R = (I_1 + I_3)(I_2 + I_3) \subseteq I_1I_2 + I_3.$$

Thus I_1I_2 and I_3 are relatively prime.

5. See (2.6.9).
6. Assume that R is not a field, equivalently, $\{0\}$ is not a maximal ideal. Thus by (7.6.9), every maximal ideal is invertible.
7. Let r be a nonzero element of R such that $rK \subseteq R$, hence $K \subseteq r^{-1}R \subseteq K$. Thus $K = r^{-1}R$. Since $r^{-2} \in K$ we have $r^{-2} = r^{-1}s$ for some $s \in R$. But then $r^{-1} = s \in R$, so $K \subseteq R$ and consequently $K = R$.
8. $R = R^r = (P_1 + P_2)^r \subseteq P_1^r + P_2$. Thus P_1^r and P_2 are relatively prime for all $r \geq 1$. Assuming inductively that P_1^r and P_2^s are relatively prime, we have

$$P_2^s = P_2^s R = P_2^s(P_1^r + P_2) \subseteq P_1^r + P_2^{s+1}$$

so

$$R = P_1^r + P_2^s \subseteq P_1^r + (P_1^r + P_2^{s+1}) = P_1^r + P_2^{s+1}$$

completing the induction.

Section 7.7

1. By Section 7.3, Problem 1, the norms are 6, 6, 4 and 9. Now if $x = a + b\sqrt{-5}$ and $x = yz$, then $N(x) = a^2 + 5b^2 = N(y)N(z)$. The only algebraic integers of norm 1 are ± 1 , and there are no algebraic integers of norm 2 or 3. Thus there cannot be a nontrivial factorization of $1 \pm \sqrt{-5}$, 2 or 3.
2. If $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$, take norms to get $(a^2 + 5b^2)(c^2 + 5d^2) = 1$, so $b = d = 0$, $a = \pm 1$, $c = \pm 1$.
3. By Problem 2, if two factors are associates, then the quotient of the factors is ± 1 , which is impossible.
4. This is a nice application of the principle that divides means contains. The greatest common divisor is the smallest ideal containing both I and J , that is, $I + J$. The least common multiple is the largest ideal contained in both I and J , which is $I \cap J$.
5. If I is a fractional ideal, then by (7.7.1) there is a fractional ideal I' such that $II' = R$. By definition of fractional ideal, there is a nonzero element $r \in R$ such that rI' is an integral ideal. If $J = rI'$, then $IJ = Rr$, a principal ideal of R .
6. This is done just as in Problems 1-3, using the factorization $18 = (2)(3^2) = (1 + \sqrt{-17})(1 - \sqrt{-17})$.
7. By (7.2.2), the algebraic integers are of the form $a + b\sqrt{-3}$, $a, b \in \mathbb{Z}$, or $\frac{u}{2} + \frac{v}{2}\sqrt{-3}$ where

u and v are odd integers. If we require that the norm be 1, we only get ± 1 in the first case. But in the second case, we have $u^2 + 3v^2 = 4$, so $u = \pm 1, v = \pm 1$. Thus if $\omega = e^{i2\pi/3}$, the algebraic integers of norm 1 are $\pm 1, \pm\omega$, and $\pm\omega^2$.

Section 7.8

1. If Rx and Ry belong to $P(R)$, then $(Rx)(Ry)^{-1} = (Rx)(Ry^{-1}) = Rxy^{-1} \in P(R)$, and the result follows from (1.1.2).
2. If $C(R)$ is trivial, then every integral ideal I of R is a principal fractional ideal $Rx, x \in K$. But $I \subseteq R$, so $x = 1x$ must belong to R , proving that R is a PID. The converse holds because every principal ideal is a principal fractional ideal.
3. $1 - \sqrt{-5} = 2 - (1 + \sqrt{-5}) \in P_2$, so $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in P_2^2$.
4. Since $2 \in P_2$, it follows that $4 \in P_2^2$, so by Problem 3, $2 = 6 - 4 \in P_2^2$.
5. $(2, 1 + \sqrt{-5})(2, 1 + \sqrt{-5}) = (4, 2(1 + \sqrt{-5}), (1 + \sqrt{-5})^2)$, and $(1 + \sqrt{-5})^2 = -4 + 2\sqrt{-5}$. Thus each of the generators of the ideal P_2^2 is divisible by 2, hence belongs to (2). Therefore $P_2^2 \subseteq (2)$.
6. $x^2 + 5 \equiv (x + 1)(x - 1) \pmod{3}$, which suggests that $(3) = P_3P'_3$, where $P_3 = (3, 1 + \sqrt{-5})$ and $P'_3 = (3, 1 - \sqrt{-5})$.
7. $P_3P'_3 = (3, 3(1 - \sqrt{-5}), 3(1 + \sqrt{-5}), 6) \subseteq (3)$ since each generator of $P_3P'_3$ is divisible by 3. But $3 \in P_3 \cap P'_3$, hence $9 \in P_3P'_3$, and therefore $9 - 6 = 3 \in P_3P'_3$. Thus $(3) \subseteq P_3P'_3$, and the result follows.

Section 7.9

1. Using (1), the product is $z = 4 + 2p + 4p^2 + p^3 + p^4$. But $4 = 3 + 1 = 1 + p$ and $4p^2 = p^2 + 3p^2 = p^2 + p^3$. Thus $z = 1 + 3p + p^2 + 2p^3 + p^4 = 1 + 2p^2 + 2p^3 + p^4$. Using (2), we are multiplying $x = \{2, 5, 14, 14, \dots\}$ by $y = \{2, 2, 11, 11, \dots\}$. Thus $z_0 = 4, z_1 = 10, z_2 = 154, z_3 = 154, z_4 = 154$, and so on. But $4 \equiv 1 \pmod{3}, 10 \equiv 1 \pmod{9}, 154 \equiv 19 \pmod{27}, 154 \equiv 73 \pmod{81}, 154 \equiv 154 \pmod{243}$. The standard form is $\{1, 1, 19, 73, 154, 154, \dots\}$. As a check, the product is $(2+3+9)(2+9)=154$, whose base 3 expansion is $1 + 0(3) + 2(9) + 2(27) + 1(81)$ as found above.
2. We have $a_0 = -1$ and $a_n = 0$ for $n \geq 1$; equivalently, $x_n = -1$ for all n . In standard form, $x_0 = p - 1, x_1 = p^2 - 1, x_2 = p^3 - 1, \dots$. Since $(p^r - 1) - (p^{r-1} - 1) = (p - 1)(p^{r-1})$, the series representation is

$$(p - 1) + (p - 1)p + (p - 1)p^2 + \dots + (p - 1)p^n + \dots$$

The result can also be obtained by multiplying by -1 on each side of the equation

$$1 = (1 - p)(1 + p + p^2 + \dots).$$

3. Let x be a nonzero element of $GF(q)$. By (6.4.1), $x^{q-1} = 1$, so $|x|^{q-1} = 1$. Thus $|x|$ is a root of unity, and since absolute values are nonnegative real, we must have $|x| = 1$, and the result follows.
4. If the absolute value is nonarchimedean, then S is bounded by (7.9.6). If the absolute value is archimedean, then by (7.9.6), $|n| > 1$ for some n . But then $|n^k| = |n|^k \rightarrow \infty$ as $k \rightarrow \infty$. Therefore S is unbounded.
5. A field of prime characteristic p has only finitely many integers $0, 1, \dots, p - 1$. Thus the set S of Problem 4 must be bounded, so the absolute value is nonarchimedean.
6. The “only if” part is handled just as in calculus. For the “if” part, note that by (iv) of (7.9.5), we have $|z_m + z_{m+1} + \dots + z_n| \leq \max\{|z_i| : m \leq i \leq n\} \rightarrow 0$ as $m, n \rightarrow \infty$. Thus the n^{th} partial sums form a Cauchy sequence, which must converge to an element in \mathbb{Q}_p .
7. Since $n! = 1 \cdot 2 \cdot \dots \cdot p \cdot \dots \cdot 2p \cdot \dots \cdot 3p \cdot \dots$, it follows from (7.9.2) and (7.9.3) that if $rp \leq n < (r + 1)p$, then $|n!| = 1/p^r$. Thus $|n!| \rightarrow 0$ as $n \rightarrow \infty$.
8. No. Although $|p^r| = 1/p^r \rightarrow 0$ as $r \rightarrow \infty$, all integers n such that $rp < n < (r + 1)p$

have p -adic absolute value 1, by (7.9.2). Thus the sequence of absolute values $|n|$ cannot converge, hence the sequence itself cannot converge.

Section 8.1

1. If $x \in V$ and $f_1(x) \neq 0$, then $f_2(x)$ must be 0 since $f_1 f_2 \in I(V)$; the result follows.
2. By Problem 1, $V \subseteq V(f_1) \cup V(f_2)$. Thus

$$V = (V \cap V(f_1)) \cup (V \cap V(f_2)) = V_1 \cup V_2.$$

Since $f_1 \notin I(V)$, there exists $x \in V$ such that $f_1(x) \neq 0$. Thus $x \notin V_1$, so $V_1 \subset V$; similarly, $V_2 \subset V$.

3. $I(V) \supseteq I(W)$ by (4). If $I(V) = I(W)$, let $V = V(S)$, $W = V(T)$. Then $IV(S) = IV(T)$, and by applying V to both sides, we have $V = W$ by (6).
4. Let $x \in V$; if $f_1(x) \neq 0$, then since $f_1 \in I(V_1)$, we have $x \notin V_1$. But then $x \in V_2$, and therefore $f_2(x) = 0$ (since $f_2 \in I(V_2)$). Thus $f_1 f_2 = 0$ on V , so $f_1 f_2 \in I(V)$.
5. If V is reducible, then V is the union of proper subvarieties V_1 and V_2 . If V_1 is reducible, then it too is the union of proper subvarieties. This decomposition process must terminate in a finite number of steps, for otherwise by Problems 1-4, there would be a strictly increasing infinite sequence of ideals, contradicting the fact that $k[X_1, \dots, X_n]$ is Noetherian.
6. If $V = \bigcup_i V_i = \bigcup_j W_j$, then $V_i = \bigcup_j (V_i \cap W_j)$, so by irreducibility, $V_i = V_i \cap W_j$ for some j . Thus $V_i \subseteq W_j$, and similarly $W_j \subseteq V_k$ for some k . But then $V_i \subseteq V_k$, hence $i = k$ (otherwise we would have discarded V_i). Thus each V_i can be paired with a corresponding W_j , and vice versa.
7. By hypothesis, $A^n = \cup(A^n \setminus V(I_i))$. Taking complements, we have $\cap V(I_i) = \emptyset$. But by (8.1.2), $\cap V(I_i) = V(\cup I_i) = V(I)$, so by the weak Nullstellensatz, $I = k[X_1, \dots, X_n]$. Thus the constant polynomial 1 belongs to I .
8. Suppose that the open sets $A^n \setminus V(I_i)$ cover A^n . By Problem 7, $1 \in I$, hence 1 belongs to a finite sum $\sum_{i \in F} I_i$. Since 1 never vanishes, $V(\sum_{i \in F} I_i) = \emptyset$. By (8.1.2), $\cap_{i \in F} V_i = \emptyset$, where $V_i = V(I_i)$. Taking complements, we have $\cup_{i \in F} (A^n \setminus V_i) = A^n$. Thus the original open covering of A^n has a finite subcovering, proving compactness.

Section 8.2

1. If $a \notin (a_1, \dots, a_k)$, then g or some other element of I would extend the inductive process to step $k + 1$.
2. In going from d_i to d_{i+1} we are taking the minimum of a smaller set.
3. By minimality of m , $a \notin (a_1, \dots, a_{m-1})$, hence f_m and g satisfy conditions 1 and 2. By choice of f_m we have $d_m \leq d$. (If $m = 1$, then $d_1 \leq d$ by choice of f_1 .)
4. Let f be the unique ring homomorphism from $R[X_1, \dots, X_n]$ to S such that f is the identity on R and $f(X_i) = x_i$, $i = 1, \dots, n$. (For example, if $a \in R$, then $aX_1^2 X_4^7 \rightarrow ax_1^2 x_4^7$.) Since the image of f contains R and $\{x_1, \dots, x_n\}$, f is surjective and the result follows.
5. By the Hilbert basis theorem, $R[X_1, \dots, X_n]$ is a Noetherian ring, hence a Noetherian $R[X_1, \dots, X_n]$ -module. By (7.5.7), S is a Noetherian $R[X_1, \dots, X_n]$ -module. But the submodules of S considered as an $R[X_1, \dots, X_n]$ -module coincide with the submodules of S as an S -module. (See Section 4.2, Problems 6 and 7; note that the kernel of the homomorphism f of Problem 4 annihilates S .) Thus S is a Noetherian S -module, that is, a Noetherian ring.

Section 8.3

1. Suppose that $xy \in J$ with $x \notin J$ and $y \notin J$. By maximality of J , the ideal $J + (x)$ contains an element $s \in S$. Similarly, $J + (y)$ contains an element $t \in S$. But then $st \in (J + (x))(J + (y)) \subseteq J + (xy) \subseteq J$, so $S \cap J \neq \emptyset$, a contradiction.
2. Let $S = \{1, f, f^2, \dots, f^r, \dots\}$. Then $I \cap S = \emptyset$ since $f \notin \sqrt{I}$. By Problem 1, I is contained in a prime ideal P disjoint from S . But $f \in S$, so f cannot belong to P , and the result follows.
3. The "if" part follows because f and f^r have the same zero-set. Conversely, if $V(f) =$

$V(g)$, then by the Nullstellensatz, $\sqrt{(f)} = \sqrt{(g)}$, and the result follows.

4. $W \subseteq V$ since $(t^4)^2 = (t^3)(t^5)$ and $(t^5)^2 = (t^3)^2(t^4)$; $L \subseteq V$ by direct verification. Conversely, if $y^2 = xz$ and $z^2 = x^2y$, let $t = y/x$. (If $x = 0$, then $y = z = 0$ and we can take $t = 0$.) Then $z = y^2/x = (y/x)^2x = t^2x$, and $z^2 = x^2y$. Therefore $z^2 = t^4x^2 = x^2y$, hence $y = t^4$. If $t = 0$ then $y = 0$, hence $z = 0$ and $(x, y, z) \in L$. Thus assume $t \neq 0$. But then $x = y/t = t^3$ and $z = t^2x = t^5$.

5. We will show that $I(V)$ is a prime ideal (see the exercises in Section 8.1). If $fg \in I(V)$, then fg vanishes on V . Using the parametric form, we have $f(t, t^2, t^3)g(t, t^2, t^3) = 0$ for all complex numbers t . Since we are now dealing with polynomials in only one variable, either $f(t, t^2, t^3) = 0$ for all t or $g(t, t^2, t^3) = 0$ for all t . Thus $f \in I(V)$ or $g \in I(V)$.

6. (a) $x = 2t/(t^2 + 1)$, $y = (t^2 - 1)/(t^2 + 1)$

(b) $x = t^2$, $y = t^3$

(c) $x = t^2 - 1$, $y = t(t^2 - 1)$

7. (Following Shafarevich, Basic Algebraic Geometry, Vol.1, page 2.) We can assume that x appears in f with positive degree. Viewing f and g as polynomials in $k(y)[x]$, a PID, f is still irreducible because irreducibility over an integral domain implies irreducibility over the quotient field. If $g = fh$ where h is a polynomial in x with coefficients in $k(y)$, then by clearing denominators we see that f must divide g in $k[x, y]$, a contradiction. (Since f is irreducible, it must either divide g or a polynomial in y alone, and the latter is impossible because x appears in f .) Thus f does not divide g in $k(y)[x]$. Since f and g are relatively prime, there exist $s, t \in k(y)[x]$ such that $fs + gt = 1$. Clearing denominators, we get $u, v \in k[x, y]$ such that $fu + gv = a$, where a is a nonzero polynomial in y alone. Now if $\alpha, \beta \in k$ and $f(\alpha, \beta) = g(\alpha, \beta) = 0$, then $a(\beta) = 0$, and this can only happen for finitely many β . For any fixed β , consider $f(x, \beta) = 0$. If this polynomial in x is not identically 0, then there are only finitely many α such that $f(\alpha, \beta) = 0$, and we are finished. Thus assume $f(x, \beta) \equiv 0$. Then $f(x, y) = f(x, y) - f(x, \beta) = (y - \beta)h$ in $k(x)[y]$, contradicting the irreducibility of f .

Section 8.4

1. Since $f = 0$ iff some $f_i = 0$, $V(f)$ is the union of the $V(f_i)$. Since each f_i is irreducible, the ideal $I_i = (f_i)$ is prime by (2.6.1), hence $V(I_i) = V(f_i)$ is an irreducible subvariety of $V(f)$. [See the problems in Section 8.1, along with the Nullstellensatz and the fact that every prime ideal is a radical ideal (Section 8.3, Problem 2).] No other decomposition is possible, for if $V(f_i) \subseteq V(f_j)$, then $(f_i) \supseteq (f_j)$. This is impossible if f_i and f_j are distinct irreducible factors of f .

2. By the Nullstellensatz, $IV(f) = \sqrt{(f)}$, and we claim that $\sqrt{(f)} = (f_1 \cdots f_r)$. For if $g \in (f_1 \cdots f_r)$, then a sufficiently high power of g will belong to (f) . Conversely, if $g^m = hf$, then each f_i divides g^m , and since the f_i are irreducible, each f_i divides g , so $(f_1 \cdots f_r)$ divides g .

3. By Problem 1, f is irreducible if and only if $V(f)$ is an irreducible hypersurface. If f and g are irreducible and $V(f) = V(g)$, then as in Problem 1, $(f) = (g)$, so $f = cg$ for some nonzero constant c (Section 2.1, Problem 2). Thus $f \rightarrow V(f)$ is a bijection between irreducible polynomials and irreducible hypersurfaces, if the polynomials f and $cf, c \neq 0$, are identified.

4. This follows from the definition of $I(X)$ in (8.1.3), and the observation that a function vanishes on a union of sets iff it vanishes on each of the sets.

5. By Section 8.1, Problem 5, every variety V is the union of finitely many irreducible subvarieties V_1, \dots, V_r . By Problem 4, $I(V) = \bigcap_{i=1}^r I(V_i)$. By the Problems in Section 8.1, each $I(V_i)$ is a prime ideal. By (8.4.3), every radical ideal is $I(V)$ for some variety V , and the result follows.

6. By Section 8.1, Problem 6, and the inclusion-reversing property of I (part (4) of (8.1.3)), the decomposition is unique if we discard any prime ideal that properly contains another one. In other words, we retain only the minimal prime ideals.

7. If f is any irreducible factor of any of the f_i , then f does not divide g . Thus for some

$j \neq i$, f does not divide f_j . By Problem 7 of Section 8.3, the simultaneous equations $f = f_j = 0$ have only finitely many solutions, and consequently X is a finite set.

8. With notation as in Problem 7, $f_i = gh_i$, where the gcd of the h_i is constant. Thus X is the union of the algebraic curve defined by $g = 0$ and the finite set defined by $h_1 = \cdots = h_m = 0$. (This analysis does not apply when X is defined by the zero polynomial, in which case $X = A^2$.)

9. If $k = \mathbb{R}$, the zero-set of $x^2 + y^{2n}$ is $\{(0, 0)\}$ for all $n = 1, 2, \dots$. If k is algebraically closed, then as a consequence of the Nullstellensatz, $V(f) = V(g)$ with f and g irreducible implies that $f = cg$ for some constant c . (See Problem 3).

10. Let $k = \mathbb{F}_2$, and let I be the ideal of $k[X]$ generated by $f(X) = X^2 + X + 1$. Since f is irreducible, I is a maximal ideal (Section 3.1, Problem 8), in particular, I is proper. But $f(0)$ and $f(1)$ are nonzero, so $V(I)$ is empty, contradicting the weak Nullstellensatz.

Section 8.5

1. If $x \notin M$, then the ideal generated by M and x is R , by maximality of M . Thus there exists $y \in M$ and $z \in R$ such that $y + zx = 1$. By hypothesis, zx , hence x , is a unit. Take the contrapositive to conclude that every nonunit belongs to M .

2. Any additive subgroup of the cyclic additive group of \mathbb{Z}_{p^n} must consist of multiples of some power of p , and it follows that every ideal is contained in (p) , which must therefore be the unique maximal ideal.

3. No. A can be nilpotent, that is, some power of A can be 0. The set will be multiplicative if A is invertible.

4. $S^{-1}(gf)$ takes m/s to $g(f(m))/s$, as does $S^{-1}gS^{-1}f$. If f is the identity on M , then $S^{-1}f$ is the identity on $S^{-1}M$.

5. By hypothesis, $gf = 0$, so $S^{-1}gS^{-1}f = S^{-1}gf = S^{-1}0 = 0$. Thus $\text{im } S^{-1}f \subseteq \ker S^{-1}g$. Conversely, let $x \in N$, $s \in S$, with $x/s \in \ker S^{-1}g$. Then $g(x)/s = 0/1$, so for some $t \in S$ we have $tg(x) = g(tx) = 0$. Therefore $tx \in \ker g = \text{im } f$, so $tx = f(y)$ for some $y \in M$. We now have $x/s = f(y)/st = (S^{-1}f)(y/st) \in \text{im } S^{-1}f$.

6. The set of nonunits is $M = \{f/g : g(a) \neq 0, f(a) = 0\}$, which is an ideal. By (8.5.9), R is a local ring with maximal ideal M .

7. The sequence $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ is exact, so by Problem 5, $0 \rightarrow N_S \rightarrow M_S \rightarrow (M/N)_S \rightarrow 0$ is exact. (If f is one of the maps in the first sequence, the corresponding map in the second sequence is $S^{-1}f$.) It follows from the definition of localization of a module that $N_S \leq M_S$, and by exactness of the second sequence we have $(M/N)_S \cong M_S/N_S$, as desired.

Section 8.6

1. If x^m belongs to the intersection of the I_i , then x belongs to each $\sqrt{I_i}$, so $x \in \bigcap_{i=1}^n \sqrt{I_i}$. Conversely, if $x \in \bigcap_{i=1}^n \sqrt{I_i}$, let $x^{m_i} \in I_i$. If m is the maximum of the m_i , then $x^m \in \bigcap_{i=1}^n I_i$, so $x \in \sqrt{\bigcap_{i=1}^n I_i}$.

2. We are essentially setting $X = Z = 0$ in R , and this collapses R down to $k[Y]$. Formally, map $f + I$ to $g + I$, where g consists of those terms in f that do not involve X or Z . Then $R/P \cong k[Y]$, an integral domain. Therefore P is prime.

3. $(X + I)(Y + I) = Z^2 + I \in P^2$, but $X + I \notin P^2$ and $Y + I \notin \sqrt{P^2} = P$.

4. P_1 is prime because $R/P_1 \cong k[Y]$, an integral domain. P_2 is maximal by (8.3.1), so P_2^2 is P_2 -primary by (8.6.6). The radical of Q is P_2 , so by (8.6.5), Q is P_2 -primary.

5. The first assertion is that

$$(X^2, XY) = (X) \cap (X, Y)^2 = (X) \cap (X^2, XY, Y^2)$$

and the second is

$$(X^2, XY) = (X) \cap (X^2, Y).$$

In each case, the left side is contained in the right side by definition of the ideals involved. The inclusion from right to left follows because if $f(X, Y)X = g(X, Y)Y^2$ (or $f(X, Y)X =$

$g(X, Y)Y$), then $g(X, Y)$ must involve X and $f(X, Y)$ must involve Y . Thus $f(X, Y)X$ is a polynomial multiple of XY .

6. By (8.6.9), a proper ideal I can be expressed as the intersection of finitely many primary ideals Q_i . If Q_i is P_i -primary, then by Problem 1,

$$I = \sqrt{I} = \cap_i \sqrt{Q_i} = \cap_i P_i.$$

7. Since X^3 and Y^n belong to I_n , we have $X, Y \in \sqrt{I_n}$, so $(X, Y) \subseteq \sqrt{I_n}$. By (8.3.1), (X, Y) is a maximal ideal. Since $\sqrt{I_n}$ is proper (it does not contain 1), we have $(X, Y) = \sqrt{I_n}$. By (8.6.5), I_n is primary.

Section 8.7

1. $[(x, y + y') + G] - [(x, y) + G] - [(x, y') + G] = 0$ since $(x, y + y') - (x, y) - (x, y') \in G$; $r[(x, y) + G] - [(rx, y) + G] = 0$ since $r(x, y) - (rx, y) \in G$; the other cases are similar.

2. Let a and b be integers such that $am + bn = 1$. If $x \in \mathbb{Z}_m$ and $y \in \mathbb{Z}_n$, then $x \otimes y = 1(x \otimes y) = a(mx \otimes y) + b(x \otimes ny) = 0$ since $z \otimes 0 = 0 \otimes z = 0$.

3. Let A be a torsion abelian group, that is, each element of A has finite order. If $x \in A$ and $y \in \mathbb{Q}$, then $nx = 0$ for some positive integer n . Thus $x \otimes y = n(x \otimes (y/n)) = nx \otimes (y/n) = 0 \otimes (y/n) = 0$.

4. We have $h = g'h' = g'gh$ and $h' = gh = gg'h'$. But if $P = T$ and $f = h$, then $g = 1_T$ makes the diagram commute, as does $g'g$. By the uniqueness requirement in the universal mapping property, we must have $g'g = 1_T$, and similarly $gg' = 1_{T'}$. Thus T and T' are isomorphic.

5. $n \otimes x = n(1 \otimes x) = 1 \otimes nx = 1 \otimes 0 = 0$.

6. $n\mathbb{Z} \otimes \mathbb{Z}_n \cong \mathbb{Z} \otimes \mathbb{Z}_n \cong \mathbb{Z}_n$ by (8.7.6), with $n \otimes x \rightarrow 1 \otimes x \rightarrow x$, and since $x \neq 0$, $n \otimes x$ cannot be 0.

7. We have a bilinear map $(f, g) \rightarrow f \otimes g$ from $\text{Hom}_R(M, M') \times \text{Hom}_R(N, N')$ to $\text{Hom}_R(M \otimes_R N, M' \otimes_R N')$, and the result follows from the universal mapping property of tensor products.

8. In terms of matrices, we are to prove that $M_m(R) \otimes M_n(R) \cong M_{mn}(R)$. This follows because $M_t(R)$ is a free R -module of rank t^2 .

Section 8.8

1. $y_1 \cdots (y_i + y_j) \cdots (y_i + y_j) \cdots y_p = y_1 \cdots y_i \cdots y_i \cdots y_p + y_1 \cdots y_i \cdots y_j \cdots y_p + y_1 \cdots y_j \cdots y_i \cdots y_p + y_1 \cdots y_j \cdots y_j \cdots y_p$. The left side, as well as the first and last terms on the right, are zero by definition of N . Thus $y_1 \cdots y_i \cdots y_j \cdots y_p = -y_1 \cdots y_j \cdots y_i \cdots y_p$, as asserted.

2. If π is any permutation of $\{a, \dots, b\}$, then by Problem 1,

$$x_{\pi(a)} \cdots x_{\pi(b)} = (\text{sgn } \pi) x_a \cdots x_b.$$

The left side will be $\pm x_a \cdots x_b$, regardless of the particular permutation π , and the result follows.

3. The multilinear map f induces a unique $h : M^{\otimes p} \rightarrow Q$ such that $h(y_1 \otimes \cdots \otimes y_p) = f(y_1, \dots, y_p)$. Since f is alternating, the kernel of h contains N , so the existence and uniqueness of the map g follows from the factor theorem.

4. By Problem 3, there is a unique R -homomorphism $g : \Lambda^n M \rightarrow R$ such that $g(y_1 \cdots y_n) = f(y_1, \dots, y_n)$. In particular, $g(x_1 \cdots x_n) = f(x_1, \dots, x_n) = 1 \neq 0$. Thus $x_1 \cdots x_n \neq 0$. If r is any nonzero element of R , then $g(rx_1 x_2 \cdots x_n) = f(rx_1, \dots, x_n) = r$, so $rx_1 \cdots x_n \neq 0$. By Problem 2, $\{x_1 \cdots x_n\}$ is a basis for $\Lambda^n M$.

5. Fix the set of indices I_0 and its complementary set J_0 . If $\sum_I a_I x_I = 0$, $x_I \in R$, multiply both sides on the right by x_{J_0} . If $I \neq I_0$, then $x_I x_{J_0} = 0$ by definition of N . Thus $a_{I_0} x_{I_0} x_{J_0} = \pm a_{I_0} x_1 \cdots x_n = 0$. By Problem 4, $a_{I_0} = 0$. Since I_0 is arbitrary, the result follows.

6. We have $R_0 \subseteq S$ by definition of S . Assume that $R_m \subseteq S$ for $m = 0, 1, \dots, n-1$, and let $a \in R_n$ ($n > 0$). Then $a \in I$, so $a = \sum_{i=1}^r c_i x_i$ where (since $x_i \in R_{n_i}$ and R is the direct sum of the R_m) $c_i \in R_{n-n_i}$. By induction hypothesis, $c_i \in S$, and since $x_i \in S$ by definition of S , we have $a \in S$, completing the induction.
7. The “if” part follows from Section 8.2, Problem 5, so assume R Noetherian. Since $R_0 \cong R/I$, it follows that R_0 is Noetherian. Since R is Noetherian, I is finitely generated, so by Problem 6, $R = S$, a finitely generated R_0 -algebra.

Section 9.1

1. Assume R is simple, and let $x \in R, x \neq 0$. Then Rx coincides with R , so $1 \in Rx$. Thus there is an element $y \in R$ such that $yx = 1$. Similarly, there is an element $z \in R$ such that $zy = 1$. Therefore

$$z = z1 = zyx = 1x = x, \text{ so } xy = zy = 1$$

and y is a two-sided inverse of x . Conversely, assume that R is a division ring, and let x be a nonzero element of the left ideal I . If y is the inverse of x , then $1 = yx \in I$, so $I = R$ and R is simple.

2. I is proper because $f(1) = x \neq 0$, and $R/I \cong Rx$ by the first isomorphism theorem.
3. The “if” part follows from the correspondence theorem, so assume that M is simple. If x is a nonzero element of M , then $M = Rx$ by simplicity. If $I = \ker f$ as in Problem 2, then $M \cong R/I$, and I is maximal by the correspondence theorem.
4. The “only if” part was done in Problem 3, so assume that M is not simple. Let N be a submodule of M with $0 < N < M$. If x is a nonzero element of N , then $Rx \leq N < M$, so x cannot generate M .
5. By Problem 3, a simple \mathbb{Z} -module is isomorphic to \mathbb{Z}/I , where I is a maximal ideal of \mathbb{Z} . By Section 2.4, Problems 1 and 2, $I = (p)$ where p is prime.
6. As in Problem 5, a simple $F[X]$ -module is isomorphic to $F[X]/(f)$, where f is an irreducible polynomial in $F[X]$. (See Section 3.1, Problem 8.)
7. If x is a nonzero element of V and y an arbitrary element of V , there is an endomorphism f such that $f(x) = y$. Therefore $V = (\text{End}_k V)x$. By Problem 4, V is a simple $\text{End}_k(V)$ -module.
8. By (4.7.4), every such short exact sequence splits iff for any submodule $N \leq M$, $M \cong N \oplus P$, where the map $N \rightarrow M$ can be identified with inclusion and the map $M \rightarrow P$ can be identified with projection. In other words, every submodule of M is a direct summand. Equivalently, by (9.1.2), M is semisimple.

Section 9.2

1. Unfortunately, multiplication by r is not necessarily an R -endomorphism of M , since $r(sx) = (rs)x$, which need not equal $s(rx) = (sr)x$.
2. Let x be a generator of M , and define $f : R \rightarrow M$ by $f(r) = rx$. By the first isomorphism theorem, $M \cong R/\text{ann } M$. The result follows from the correspondence theorem.
3. Let $M = \mathbb{Z}_p \oplus \mathbb{Z}_p$ where p is prime. Then M is not a simple \mathbb{Z} -module, but $\text{ann } M = p\mathbb{Z}$ is a maximal ideal of \mathbb{Z} .
4. The computation given in the statement of the problem shows that $(1,0)$ is a generator of V , hence V is cyclic. But $N = \{(0, b) : b \in F\}$ is a nontrivial proper submodule of V . (Note that $T(0, b) = (0, 0) \in N$.) Therefore V is not simple.
5. Since F is algebraically closed, f has an eigenvalue $\lambda \in F$. Thus the kernel of $f - \lambda I$ is not zero, so it must be all of M . Therefore $f(m) = \lambda m$ for all $m \in M$.
6. If $r \in I$ and $s + I \in R/I$, then $r(s + I) = rs + I$. But if I is not a right ideal, we cannot guarantee that rs belongs to I .

Section 9.3

1. For each $j = 1, \dots, n$, there is a finite subset $I(j)$ of I such that x_j belongs to the direct sum of the $M_i, i \in I(j)$. If J is the union of the $I(j)$, then $M \subseteq \bigoplus_{i \in J} M_i \subseteq M$, so M is the

direct sum of the $M_i, i \in J$.

2. Each simple module $M_i, i = 1, \dots, n$, is cyclic (Section 9.1, Problem 4), and therefore can be generated by a single element x_i . Thus M is generated by x_1, \dots, x_n .
3. A left ideal is simple iff it is minimal, so the result follows from (9.1.2).
4. No. If it were, then by Section 9.1, Problem 5, \mathbb{Z} would be a direct sum of cyclic groups of prime order. Thus each element of \mathbb{Z} would have finite order, a contradiction.
5. By (4.6.4), every finite abelian group is the direct sum of various \mathbb{Z}_p, p prime. If p and q are distinct primes, then $\mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ by the Chinese remainder theorem. Thus \mathbb{Z}_n can be assembled from cyclic groups of prime order as long as no prime appears more than once in the factorization of n . (If $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is part of the decomposition, the group cannot be cyclic.) Consequently, \mathbb{Z}_n is semisimple if and only if n is square-free.
6. This follows from Section 9.1, Problem 8. (In the first case, B is semisimple by hypothesis, and in the second case A is semisimple. The degenerate case $M = 0$ can be handled directly.)
7. Conditions (a) and (b) are equivalent by (9.3.2) and the definition of semisimple ring. By Problem 6, (b) implies both (c) and (d). To show that (c) implies (b) and (d) implies (b), let M be a nonzero R -module, with N a submodule of M . By hypothesis, the sequence $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ splits. (By hypothesis, M/N is projective in the first case and N is injective in the second case.) By Section 9.1, Problem 8, M is semisimple.

Section 9.4

1. If there is an infinite descending sequence $I_1 \supset I_2 \supset \dots$ of left ideals, we can proceed exactly as in (9.4.7) to reach a contradiction.
2. Let I_1 be any nonzero left ideal. If I_1 is simple, we are finished. If not, there is a nonzero left ideal I_2 such that $I_1 \supset I_2$. If we continue inductively, the Artinian hypothesis implies that the process must terminate in a simple left ideal I_t .
3. By Problem 2, the ring R has a simple R -module M . The hypothesis that R has no nontrivial two-sided ideals implies that we can proceed exactly as in (9.4.6) to show that M is faithful.
4. If V is infinite-dimensional over D , then exactly as in (9.4.7), we find an infinite descending chain of left ideals, contradicting the assumption that R is Artinian.
5. By Problem 4, V is a finite-dimensional vector space over D , so we can reproduce the discussion preceding (9.4.7) to show that $R \cong \text{End}_D(V) \cong M_n(D^o)$.
6. The following is a composition series:

$$0 < M_1 < M_1 \oplus M_2 < \dots < M_1 \oplus M_2 \oplus \dots \oplus M_n = M.$$

7. By (9.1.2), M is a direct sum of simple modules. If the direct sum is infinite, then we can proceed as in Problem 6 to construct an infinite ascending (or descending) chain of submodules of M , contradicting the hypothesis that M is Artinian and Noetherian.

Section 9.5

1. If $g \in \ker \rho$, then $gv = v$ for every $v \in V$. Take $v = 1_G$ to get $g1_G = 1_G$, so $g = 1_G$ and ρ is injective.
2. $(gh)(v(i)) = v(g(h(i)))$ and $g(h(v(i))) = g(v(h(i))) = v(g(h(i)))$. Also, $1_G(v(i)) = v(1_G(i)) = v(i)$.
3. We have $g(v(1)) = v(4)$, $g(v(2)) = v(2)$, $g(v(3)) = v(1)$, $g(v(4)) = v(3)$, so

$$[g] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

4. We have $gv_1 = v_2$, $gv_2 = v_3 = -v_1 - v_2$; $hv_1 = v_1$, $hv_2 = v_3 = -v_1 - v_2$. Thus

$$[g] = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \quad h = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}.$$

5. We have $v_1 = e_1$ and $v_2 = -\frac{1}{2}e_1 + \frac{1}{2}\sqrt{3}e_2$. Thus

$$P^{-1} = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{2}\sqrt{3} \end{bmatrix}, \quad P = \begin{bmatrix} 1 & \frac{1}{3}\sqrt{3} \\ 0 & \frac{2}{3}\sqrt{3} \end{bmatrix}$$

and

$$[g]' = P^{-1}[g]P = \begin{bmatrix} -\frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{bmatrix},$$

$$[h]' = P^{-1}[h]P = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

6. Check by direct computation that the matrices A and B satisfy the defining relations of D_8 : $A^4 = I$, $B^2 = I$, $AB = BA^{-1}$. (See Section 5.8.)

7. Yes. Again, check by direct computation that the matrices $A^i B^j$, $i = 0, 1, 2, 3$, $j = 0, 1$, are distinct. Thus if $g \in D_8$ and $\rho(g) = I$, then g is the identity element of D_8 .

Section 9.6

1. Let W be the one-dimensional subspace spanned by $v_1 + v_2 + v_3$. Since any permutation in S_3 permutes the v_i , $v \in W$ implies $gv \in W$.

2. Multiplying $[a^r]$ by $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, we have $a^r v_1 = v_1$ and $a^r v_2 = r v_1 + v_2$. Since W is spanned by v_1 , it is closed under the action of G and is therefore a kG -submodule.

3. If

$$[a^r] \begin{bmatrix} x \\ y \end{bmatrix} = c \begin{bmatrix} x \\ y \end{bmatrix}$$

then $x + ry = cx$ and $y = cy$. If $y \neq 0$ then $c = 1$, so ry , hence y , must be 0. Thus $c = 1$ and x is arbitrary, so that any one-dimensional kG -submodule must coincide with W .

4. If $V = W \oplus U$, where U is a kG -submodule, then U must be one-dimensional. By Problem 3, $W = U$, and since $W \neq 0$, this is impossible.

5. If M is semisimple and either Noetherian or Artinian, then M is the direct sum of finitely many simple modules. These simple modules are the factors of a composition series, and the result follows from (7.5.12).

6. Let e be the natural projection on M_1 . Then e is an idempotent, $e \neq 0$ since $M_1 \neq 0$, and $e \neq 1$ since $e = 0$ on M_2 and $M_2 \neq 0$.

7. Let e be a nontrivial idempotent, and define $e_1 = e$, $e_2 = 1 - e$. By direct computation, e_1 and e_2 are nontrivial idempotents that are orthogonal. Take $M_1 = e_1(M)$, $M_2 = e_2(M)$. Then M_1 and M_2 are nonzero submodules with $M = M_1 + M_2$. To show that the sum is direct, let $z = e_1 x = e_2 y \in M_1 \cap M_2$, with $x, y \in M$. Then $e_1 z = e_1 e_2 y = 0$, and similarly $e_2 z = 0$. Thus $z = 1z = e_1 z + e_2 z = 0$.

Section 9.7

1. If $M = Rx$, define $f : R \rightarrow M$ by $f(r) = rx$. By the first isomorphism theorem, $M \cong R/\ker f$. Moreover, $\ker f = \text{ann}(M)$. Conversely, R/I is cyclic since it is generated by $1 + I$.

2. If N is a maximal submodule of M , then N is the kernel of the canonical map of M onto the simple module M/N . Conversely, if $f : M \rightarrow S$, S simple, then $f(M)$ is 0 or S , so $f = 0$ or $S \cong M/\ker f$. Thus $\ker f$ is either M or a maximal submodule of M . The intersection of all kernels therefore coincides with the intersection of all maximal submodules. [If there are no maximal submodules, then the intersection of all kernels is M .]

3. By the correspondence theorem, the intersection of all maximal left ideals of R/I is 0. This follows because the intersection of all maximal left ideals of R containing I is the intersection of all maximal left ideals of R . [Note that $J(R)$ is contained in every maximal

left ideal, and $I = J(R)$.]

4. Let g be an R -module homomorphism from N to the simple R -module S . Then $gf : M \rightarrow S$, so by Problem 2, $J(M) \subseteq \ker(gf)$. But then $f(J(M)) \subseteq \ker g$. Take the intersection over all g to get $f(J(M)) \subseteq J(N)$.

5. Suppose $a \in J(R)$. If $1 + ab$ is a nonunit, then it belongs to some maximal ideal M . But then a belongs to M as well, and therefore so does ab . Thus $1 \in M$, a contradiction. Now assume $a \notin J(R)$, so that for some maximal ideal M , $a \notin M$. By maximality, $M + Ra = R$, so $1 = x + ra$ for some $x \in M$ and $r \in R$. Since x belongs to M , it cannot be a unit, so if we set $b = -r$, it follows that $1 + ab$ is a nonunit.

6. By the correspondence theorem, there is a bijection, given by $\psi(A) = A/N$, between maximal submodules of M containing N and maximal submodules of M/N . Since $N \leq J(M)$ by hypothesis, a maximal submodule of M containing N is the same thing as a maximal submodule of M . Thus $J(M)$ corresponds to $J(M/N)$, that is, $\psi(J(M)) = J(M/N)$. Since $\psi(J(M)) = J(M)/N$, the result follows.

Section 9.8

1. $a^t \in (a^{t+1})$, so there exists $b \in R$ such that $a^t = ba^{t+1}$. Since R is an integral domain we have $1 = ba$.

2. Let a be a nonzero element of the Artinian integral domain R . The sequence $(a) \supseteq (a^2) \supseteq \dots$ stabilizes, so for some t we have $(a^t) = (a^{t+1})$. By Problem 1, a has an inverse, proving that R is a field.

3. If P is a prime ideal of R , then R/P is an Artinian integral domain by (7.5.7) and (2.4.5). By Problem 2, R/P is a field, so by (2.4.3), P is maximal.

4. We have $P \cap I \in \mathcal{S}$ and $P \cap I \subseteq I$, so by minimality of I , $P \cap I = I$. Thus $P \supseteq I = \bigcap_{j=1}^n I_j$, so by (7.6.2), $P \supseteq I_j$ for some j . But P and I_j are maximal ideals, hence $P = I_j$.

5. If $z \in F$, with $z = x + y$, $x \in M$, $y \in N$, define $h : F \rightarrow M/JM \oplus N/JN$ by $h(z) = (x + JM) + (y + JN)$. Then h is an epimorphism with kernel $JM + JN = JF$, and the result follows from the first isomorphism theorem.

6. By (9.8.5), M/JM is an n -dimensional vector space over the residue field k . Since F , hence F/JF , is generated by n elements, F/JF has dimension at most n over k . Thus N/JN must have dimension zero, and the result follows.

7. Multiplication of an element of I on the right by a polynomial $f(X, Y)$ amounts to multiplication by the constant term of f . Thus I is finitely generated as a right R -module iff it is finitely generated as an abelian group. This is a contradiction, because as an abelian group,

$$I = \bigoplus_{n=0}^{\infty} \mathbb{Z}X^nY.$$

8. By the Hilbert basis theorem, $\mathbb{Z}[X]$ is a Noetherian ring and therefore a Noetherian left $\mathbb{Z}[X]$ -module. The isomorphic copy $\mathbb{Z}[X]Y$ is also a Noetherian left $\mathbb{Z}[X]$ -module, hence so is R , by (7.5.8). A left ideal of R that is finitely generated as a $\mathbb{Z}[X]$ -module is finitely generated as an R -module, so R is left-Noetherian.

9. The set $\{\bar{x}_1, \dots, \bar{x}_n\}$ spans V , and therefore contains a basis. If the containment is proper, then by (9.8.5) part (ii), $\{x_1, \dots, x_n\}$ cannot be a minimal generating set, a contradiction.

10. In vector-matrix notation we have $y = Ax$ and therefore $\bar{y} = \bar{A}\bar{x}$, where $\bar{a}_{ij} = a_{ij} + J$. By Problem 9, \bar{x} and \bar{y} are bases, so that $\det \bar{A} \neq 0$. But under the canonical map of R onto k , $\det A$ maps to $\det \bar{A}$, and therefore $\det A$ cannot belong to the kernel of the map, namely J . But by (8.5.9), J is the ideal of nonunits of R , so $\det A$ is a unit.

Section 10.1

1. This is exactly the same as the proof for groups in (1.1.1).

2. Any ring homomorphism on \mathbb{Q} is determined by its values on \mathbb{Z} (write $m = (m/n)n$ and apply the homomorphism g to get $g(m/n) = g(m)/g(n)$). Thus if $gi = hi$, then g coincides with h on \mathbb{Z} , so $g = h$, proving that i is epic.

3. Let AZB be a shorthand notation for the composition of the unique morphism from A to the zero object Z , followed by the unique morphism from Z to B . If Z' is another zero object, then $AZB = (AZ'Z)B = A(Z'ZB) = A(Z'B) = AZ'B$, as claimed.
4. If $is = it$, then $fis = fit = 0$, so $is(=it) = ih$ where h is unique. Thus s and t must coincide with h , hence i is monic.
5. A kernel of a monic $f : A \rightarrow B$ is 0 , realized as the zero map from a zero object Z to A . For $f0 = 0$, and if $fg = 0$, then $fg = f0$; since f is monic, $g = 0$. But then g can be factored through 0_{ZA} . Similarly, a cokernel of the epic $f : A \rightarrow B$ is the zero map from B to a zero object.
6. If $j = ih$ and $i = jh'$, then $i = ihh'$, so by uniqueness in part (2) of the definition of kernel (applied when $g = i$), hh' , and similarly $h'h$, must be the identity.
7. Define $h : K \rightarrow A$ by $h(x) = 1$ for all x . Since K is nontrivial, h cannot be injective, so that $g \neq h$. But $fg = fh$, since both maps take everything in K to the identity of B .
8. The kernel of a ring homomorphism is an ideal, but not a subring (since it does not contain the multiplicative identity).
9. Let $f : A \rightarrow B$ be a noninjective ring homomorphism. Let C be the set of pairs (x, y) in the direct product $A \times A$ such that $f(x) = f(y)$. Since f is not injective, there is an element (x, y) of C with $x \neq y$. Thus if $D = \{(x, x) : x \in A\}$, then $D \subset C$. If g is the projection of $A \times A$ on the first coordinate, and h is the projection on the second coordinate, then $f(g(x, y)) = f(x)$ and $f(h(x, y)) = f(y)$, so $fg = fh$ on the ring C . But g and h disagree on the nonempty set $C \setminus D$, so f is not monic.
10. Let g be the canonical map of N onto $N/f(M)$, and let $h : N \rightarrow N/f(M)$ be identically zero. Since gf sends everything to 0 , we have $gf = hf$ with $g \neq h$. Thus f is not epic.

Section 10.2

1. Suppose that y is the product of the x_i . By definition of product, if $f_i : x \rightarrow x_i$ for all i , there is a unique $f : x \rightarrow y$ such that $p_i f = f_i$. Since $p_i : y \rightarrow x_i$, we have $y \leq x_i$. Moreover, if $x \leq x_i$ for all i , then $x \leq y$. Therefore y is a greatest lower bound of the x_i .
2. No. For example, consider the usual ordering on the integers.
3. By duality, a coproduct of the x_i , if it exists, is a least upper bound.
4. If x has order r and y has order s , then $rs(x + y) = s(rx) + r(sy) = 0$. Thus the sum of two elements of finite order also has finite order, and the result follows.
5. The key point is that if f is a homomorphism of a torsion abelian group S , then $f(S)$ is also torsion [since $nf(x) = f(nx)$]. Thus in diagram (1) with $A = \prod A_i$, we have $f(S) \subseteq T(A)$. Since $\prod A_i$ is the product in the category of abelian groups, it follows that $T(A)$ satisfies the universal mapping property and is therefore the product in the category of torsion abelian groups.
6. Given homomorphisms $f_j : G_j \rightarrow H$, we must lift the f_j to a homomorphism from the free product to H . This is done via $f(a_1 \cdots a_n) = f_1(a_1) \cdots f_n(a_n)$. If i_j is the inclusion map from G_j to $*G_i$, then $f(i_j(a_j)) = f(a_j) = f_j(a_j)$, as required.
7. We have $p_i f = f_i$, where $f_i : G \rightarrow C_i$. The f_i can be chosen to be surjective (e.g., take G to be the direct product of the C_i), and it follows that the p_i are surjective.
8. Since $f : C_1 \rightarrow C$, we have $f(a_1) = na$ for some positive integer n . Thus

$$a_1 = f_1(a_1) = p_1 f(a_1) = p_1(na) = np_1(a) = na_1;$$

$$0 = f_2(a_1) = p_2 f(a_1) = p_2(na) = np_2(a) = na_2.$$

9. By Problem 8, the order of C_1 divides $n - 1$, and the order of C_2 divides n . There are many choices of C_1 and C_2 for which this is impossible. For example, let C_1 and C_2 be nontrivial p -groups for a fixed prime p .

Section 10.3

1. If $f : x \rightarrow y$, then $Ff : Fx \rightarrow Fy$. By definition of the category of preordered sets, this statement is equivalent to $x \leq y \implies Fx \leq Fy$. Thus functors are order-preserving maps.

2. F must take the morphism associated with xy to the composition of the morphism associated with Fx and the morphism associated with Fy . In other words, $F(xy) = F(x)F(y)$, that is, F is a homomorphism.
3. If $\beta \in X^*$, then $(gf)^*(\beta) = \beta gf$ and $f^*g^*(\beta) = f^*(\beta g) = \beta gf$.
4. To verify the functorial property, note that

$$(gf)^{**}(v^{**}) = v^{**}(gf)^* = v^{**}f^*g^* \text{ (by Problem 3)}$$

and

$$g^{**}f^{**}v^{**} = g^{**}(v^{**}f^*) = v^{**}f^*g^*.$$

Thus $(gf)^{**} = g^{**}f^{**}$. If f is the identity, then so is f^* , and consequently so is f^{**} .

5. $f^{**}t_V(v) = \overline{f^{**}(\bar{v})} = \bar{v}f^*$, and if $\beta \in W^*$, then $(\bar{v}f^*)(\beta) = \bar{v}(f^*\beta) = (f^*\beta)(v) = \beta f(v)$. But $t_W f(v) = \overline{f(v)}$ where $\overline{f(v)}(\beta) = \beta f(v)$.

6. Groups form a subcategory because every group is a monoid and every group homomorphism is, in particular, a monoid homomorphism. The subcategory is full because every monoid homomorphism from one group to another is also a group homomorphism.

7(a). If two group homomorphisms are the same as set mappings, they are identical as homomorphisms as well. Thus the forgetful functor is faithful. But not every map of sets is a homomorphism, so the forgetful functor is not full.

(b) Since (f, g) is mapped to f for arbitrary g , the projection functor is full but not faithful (except in some degenerate cases).

Section 10.4

1. If a homomorphism from \mathbb{Z}_2 to \mathbb{Q} takes 1 to x , then $0 = 1 + 1 \rightarrow x + x = 2x$. But 0 must be mapped to 0, so $x = 0$.
2. A nonzero homomorphism can be constructed with $0 \rightarrow 0$, $1 \rightarrow \frac{1}{2}$. Then $1 + 1 \rightarrow \frac{1}{2} + \frac{1}{2} = 1 = 0$ in \mathbb{Q}/\mathbb{Z} .
3. Since a trivial group cannot be mapped onto a nontrivial group, there is no way that Fg can be surjective.
4. Let f be a homomorphism from \mathbb{Q} to \mathbb{Z} . If r is any rational number and m is a positive integer, then

$$f(r) = f\left(\frac{r}{m} + \cdots + \frac{r}{m}\right) = mf\left(\frac{r}{m}\right)$$

so

$$f\left(\frac{r}{m}\right) = \frac{f(r)}{m}.$$

But if $f(r) \neq 0$, we can choose m such that $f(r)/m$ is not an integer, a contradiction. Therefore $f = 0$.

5. By Problem 4, $\text{Hom}(\mathbb{Q}, \mathbb{Z}) = 0$. But $\text{Hom}(\mathbb{Z}, \mathbb{Z}) \neq 0$, so as in Problem 3, Gf cannot be surjective.
6. We have $\mathbb{Z}_2 \otimes \mathbb{Z} \cong \mathbb{Z}_2$ and $\mathbb{Z}_2 \otimes \mathbb{Q} = 0$

$$\left[1 \otimes \frac{m}{n} = 1 \otimes \frac{2m}{2n} = 2 \otimes \frac{m}{2n} = 0 \otimes \frac{m}{2n} = 0.\right]$$

Thus the map Hf cannot be injective.

7. Since $f_* = Ff$ is injective, $f\alpha = 0$ implies $\alpha = 0$, so f is monic and hence injective. Since $g_*f_* = 0$, we have $gf\alpha = 0$ for all $\alpha \in \text{Hom}(M, A)$. Take $M = A$ and $\alpha = 1_A$ to conclude that $gf = 0$, so that $\text{im } f \subseteq \ker g$. Finally, take $M = \ker g$ and $\alpha : M \rightarrow B$ the inclusion map. Then $g_*\alpha = g\alpha = 0$, so $\alpha \in \ker g_* = \text{im } f_*$. Thus $\alpha = f\beta$ for some $\beta \in \text{Hom}(M, A)$. Thus $\ker g = M = \text{im } \alpha \subseteq \text{im } f$.

8. If (3) is exact for all possible R -modules N , then (1) is exact. This is dual to the result of Problem 7, and the proof amounts to interchanging injective and surjective, monic and epic, inclusion map and canonical map, kernel and cokernel.

Section 10.5

1. If $x \in P$, then $f(x)$ can be expressed as $\sum_i t_i e_i$ (a finite sum), and we define $f_i(x) = t_i$ and $x_i = \pi(e_i)$. Then

$$x = \pi(f(x)) = \pi\left(\sum_i t_i e_i\right) = \sum_i t_i \pi(e_i) = \sum_i f_i(x) x_i.$$

2. $\pi(f(x)) = \sum_i f_i(x) \pi(e_i) = \sum_i f_i(x) x_i = x$.

3. By Problem 2, the exact sequence $0 \rightarrow \ker \pi \rightarrow F \rightarrow P \rightarrow 0$ (with $\pi : F \rightarrow P$) splits, and therefore P is a direct summand of the free module F and hence projective.

4. Since R^n is free, the “if” part follows from (10.5.3), part (4). If P is projective, then by the proof of (3) implies (4) in (10.5.3), P is a direct summand of a free module of rank n . [The free module can be taken to have a basis whose size is the same as that of a set of generators for P .]

5. This follows from Problem 1 with $F = R^n$.

6. If P is projective and isomorphic to M/N , we have an exact sequence $0 \rightarrow N \rightarrow M \rightarrow P \rightarrow 0$. Since P is projective, the sequence splits by (10.5.3), part (3), so P is isomorphic to a direct summand of M . Conversely, assume that P is a direct summand of every module of which it is a quotient. Since P is a quotient of a free module F , it follows that P is a direct summand of F . By (10.5.3) part (4), P is projective.

7. In the diagram above (10.5.1), take $M = R_1 \oplus R_2$, with $R_1 = R_2 = R$. Take $P = N = R_1$, $f = 1_{R_1}$, and let g be the natural projection of M on N . Then we can take $h(r) = r + s$, $r \in R_1, s \in R_2$, where s is either 0 or r . By replacing M by an arbitrary direct sum of copies of R , we can produce two choices for the component of $h(r)$ in each R_i , $i = 2, 3, \dots$ (with the restriction that only finitely many components are nonzero). Thus there will be infinitely many possible choices for h altogether.

Section 10.6

1. $f'g(a) = (g(a), 0) + W$ and $g'f(a) = (0, f(a)) + W$, with $(g(a), 0) - (0, f(a)) = (g(a), -f(a)) \in W$. Thus $f'g = g'f$.

2. If $(b, c) \in W$, then $b = g(a), c = -f(a)$ for some $a \in A$. Therefore

$$g''(c) + f''(b) = -g''f(a) + f''g(a) = 0$$

and h is well-defined.

3. $hg'(c) = h((0, c) + W) = g''(c) + 0 = g''(c)$ and $hf'(b) = h((b, 0) + W) = 0 + f''(b) = f''(b)$.

4. $h'((b, c) + W) = h'((0, c) + W + (b, 0) + W) = h'(g'(c) + f'(b)) = h'g'(c) + h'f'(b) = g''(c) + f''(b) = h((b, c) + W)$.

5. If $f'(b) = 0$, then by definition of f' , $(b, 0) \in W$, so for some $a \in A$ we have $b = g(a)$ and $f(a) = 0$. Since f is injective, $a = 0$, hence $b = 0$ and f' is injective.

6. If $b \in B, c \in C$, then surjectivity of f gives $c = f(a)$ for some $a \in A$. Thus $f'(b + g(a)) = (b + g(a), 0) + W = (b + g(a), 0) + W + (-g(a), f(a)) + W$ [note that $(-g(a), f(a)) \in W$] $= (b, f(a)) + W = (b, c) + W$, proving that f' is surjective.

7. If $(a, c) \in D$, then $f(a) = g(c)$ and $fg'(a, c) = f(a)$, $gf'(a, c) = g(c)$. Thus $fg' = gf'$.

8. If $x \in E$, then $fg''(x) = gf''(x)$, so $(g''(x), f''(x)) \in D$. Take $h(x) = (g''(x), f''(x))$, which is the only possible choice that satisfies $g'h = g''$ and $f'h = f''$.

9. If $(a, c) \in D$ and $f'(a, c) = 0$, then $c = 0$, so $f(a) = g(c) = 0$. Since f is injective, $a = 0$. Consequently, $(a, c) = 0$ and f' is injective.

10. If $c \in C$, then there exists $a \in A$ such that $f(a) = g(c)$. Thus $(a, c) \in D$ and $f'(a, c) = c$, proving that f' is surjective.

11. If $x, y \in I$, then $f(xy) = xf(y)$ and $f(xy) = f(yx) = yf(x)$. Thus $xf(y) = yf(x)$, and if x and y are nonzero, the result follows upon division by xy .

12. We must extend $f : I \rightarrow Q$ to $h : R \rightarrow Q$. Let z be the common value $f(x)/x$, $x \in I$, $x \neq 0$. Define $h(r) = rz$, $r \in R$. Then h is an R -homomorphism, and if $x \in I$, $x \neq 0$,

then $h(x) = xz = xf(x)/x = f(x)$. Since $h(0) = f(0) = 0$, h is an extension of f and the result follows from (10.6.4).

Section 10.7

1. The only nonroutine verification is the check that $sf \in \text{Hom}_R(M, N)$:

$$(sf)(rm) = f(rms) = rf(ms) = r[(sf)(m)].$$

2. $(fr)(ms) = f(r(ms)) = f((rm)s) = f(rm)s = [(fr)(m)]s$.
3. $(sf)(mr) = s(f(mr)) = s(f(m)r) = (sf(m))r = [(sf)(m)]r$.
4. $(fr)(sm) = (f(sm))r = (sf(m))r = s(f(m)r) = s[(fr)(m)]$.
5. In Problem 2, M and N are right S -modules, so we write f on the left: $(fr)m = f(rm)$. In Problem 3, M and N are right R -modules, and we write f on the left: $(sf)m = s(fm)$. In Problem 4, M and N are left S -modules, and we write f on the right: $m(fr) = (mf)r$.
6. Let $y \in M$, $r \in R$ with $r \neq 0$. By hypothesis, $x = \frac{1}{r}y \in M$, so we have $x \in M$ such that $y = rx$, proving M divisible.
7. If $y \in M$, $r \in R$ with $r \neq 0$, we must define $\frac{1}{r}y$. Since M is divisible, there exists $x \in M$ such that $y = rx$, and we take $\frac{1}{r}y = x$. If $x' \in M$ and $y = rx'$, then $r(x - x') = 0$, and since M is torsion-free, $x = x'$. Thus x is unique and scalar multiplication is well-defined.
8. Let f be a nonzero R -homomorphism from Q to R . Then $f(u) = 1$ for some $u \in Q$. [If $f(x) = r \neq 0$, then $rf(x/r) = f(rx/r) = f(x) = r$, so we can take $u = x/r$.] Now if s is a nonzero element of R , then $sf(u/s) = f(su/s) = f(u) = 1$, so $f(u/s)$ is an inverse of s . Consequently, R is a field, contradicting the hypothesis.

Section 10.8

1. Let $A = R[X]$ where R is any commutative ring. As an R -algebra, A is generated by X , but A is not finitely generated as an R -module since it contains polynomials of arbitrarily high degree.
2. The bilinear map determined by $(X^i, Y^j) \rightarrow X^i Y^j$ induces an R -homomorphism of $R[X] \otimes_R R[Y]$ onto $R[X, Y]$, with inverse determined by $X^i Y^j \rightarrow X^i \otimes Y^j$.
3. Abbreviate X_1, \dots, X_n by X and Y_1, \dots, Y_m by Y . Let A be a homomorphic image of $R[X]$ under f , and B a homomorphic image of $R[Y]$ under g . Then $A \otimes_R B$ is a homomorphic image of $R[X] \otimes R[Y] (\cong R[X, Y]$ by Problem 2) under $f \otimes g$.
4. If $f : A \rightarrow B$ is an injective R -module homomorphism, then by hypothesis, $(1 \otimes f) : S \otimes_R A \rightarrow S \otimes_R B$ is injective. Also by hypothesis,

$$(1 \otimes (1 \otimes f)) : M \otimes_S S \otimes_R A \rightarrow M \otimes_S S \otimes_R B$$

is injective. Since $M \otimes_S S \cong M$, the result follows.

5. Let $f : A \rightarrow B$ be injective. Since $A \otimes_S S \cong A$ and $B \otimes_S S \cong B$, it follows from the hypothesis that $(f \otimes 1) : A \otimes_S (S \otimes_R M) \rightarrow B \otimes_S (S \otimes_R M)$ is injective. Thus $S \otimes_R M$ is a flat S -module.
6. α is derived from the bilinear map $S^{-1}R \times M \rightarrow S^{-1}M$ given by $(r/s, x) \rightarrow rx/s$. We must also show that β is well-defined. If $x/s = y/t$, then there exists $u \in S$ such that $utx = usy$. Thus

$$\frac{1}{s} \otimes x = \frac{ut}{sut} \otimes x = \frac{1}{sut} \otimes utx = \frac{1}{sut} \otimes usy = \frac{1}{t} \otimes y$$

as required. By construction, α and β are inverses of each other and yield the desired isomorphism.

7. We must show that $S^{-1}R \otimes_R -$ is an exact functor. But in view of Problem 6, an equivalent statement is the localization functor S^{-1} is exact, and this has already been proved in Section 8.5, Problem 5.

Section 10.9

1. The proof of (10.9.4) uses the fact that we are working in the category of modules. To simply say “duality” and reverse all the arrows, we would need an argument that did not depend on the particular category.
2. Let N be the direct limit of the N_i . The direct system $\{N_i, h(i, j)\}$ induces a direct system $\{M \otimes N_i, 1 \otimes h(i, j)\}$. Compatibility in the new system reduces to compatibility in the old system; tensoring with 1 is harmless. Since compatible maps $f_i : N_i \rightarrow B$ can be lifted to $f : N \rightarrow B$, it follows that compatible maps $g_i : M \otimes N_i \rightarrow B$ can be lifted to $g : M \otimes N \rightarrow B$. Thus $M \otimes N$ satisfies the universal mapping property for $\{M \otimes N_i\}$.
3. The direct limit is $A = \cup_{n=1}^{\infty} A_n$, with $\alpha_n : A_n \rightarrow A$ the inclusion map
5. Each R -homomorphism f from the direct sum of the A_i to B induces an R -homomorphism $f_i : A_i \rightarrow B$. [f_i is the injection of A_i into the direct sum, followed by f]. Take $\alpha(f) = (f_i, i \in I) \in \prod_i \text{Hom}_R(A_i, B)$. Conversely, given such a family $(f_i, i \in I)$, the f_i can be lifted uniquely to $\beta(f_i, i \in I) = f$. Since α and β are inverse R -homomorphisms, the result follows.
6. If $f : A \rightarrow \prod_i B_i$, define $\alpha(f) = (p_i f, i \in I) \in \prod_i \text{Hom}_R(A, B_i)$, where p_i is the projection of the direct product onto the i^{th} factor. Conversely, given $(g_i, i \in I)$, where $g_i : A \rightarrow B_i$, the g_i can be lifted to a unique $g : A \rightarrow \prod_i B_i$ such that $p_i g = g_i$ for all i . If we take $\beta(g_i, i \in I) = g$, then α and β are inverse R -homomorphisms, and the result follows.
7. There is a free module F such that $F = M \oplus M'$, and since F is torsion-free, so is M . Since M is injective, it is divisible, so by Problem 7 of Section 10.7, M is a vector space over the quotient field Q , hence a direct sum of copies of Q . Therefore, using Problem 5 above and Problem 8 of Section 10.7,

$$\text{Hom}_R(M, R) = \text{Hom}_R(\oplus Q, R) \cong \prod \text{Hom}(Q, R) = 0.$$

8. By Problem 7, $\text{Hom}_R(M, R) = 0$. Let M be a direct summand of the free module F with basis $\{r_i, i \in I\}$. If x is a nonzero element of M , then x has some nonzero coordinate with respect to the basis, say coordinate j . If p_j is the projection of F on coordinate j (the j^{th} copy of R), then p_j restricted to M is a nonzero R -homomorphism from M to R . (Note that x does not belong to the kernel of p_j .) Thus the assumption that $M \neq 0$ leads to a contradiction.