Solutions Chapters 1–5

Section 1.1

1. Under multiplication, the positive integers form a monoid but not a group, and the positive even integers form a semigroup but not a monoid.
2. With $|a|$ denoting the order of a, we have $|0| = 1$, $|1| = 6$, $|2| = 3$, $|3| = 2$, $|4| = 3$, and $|5| = 6$.
3. There is a subgroup of order $6/d$ for each divisor d of 6. We have $\mathbb{Z}_6$ itself $(d = 1)$, $\{0\}(d = 6), \{0, 2, 4\}(d = \ 2)$, and $\{0, 3\}(d = 3)$.
4. S forms a group under addition. The inverse operation is subtraction, and the zero matrix is the additive identity.
5. S^* does not form a group under multiplication, since a nonzero matrix whose determinant is 0 does not have a multiplicative inverse.
6. If d is the smallest positive integer in H, then H consists of all multiples of d. For if $x \in H$ we have $x = qd + r$ where $0 \le r < d$. But then $r = x - qd \in H$, so r must be 0.
7. Consider the rationals with addition mod 1, in other words identify rational numbers that differ by an integer. Thus, for example, $1/3 = 4/3 = 7/3$, etc. The group is infinite, but every element generates a finite subgroup. For example, the subgroup generated by $1/3$ is $\{1/3, 2/3, 0\}$.
8. $(ab)^{mn} = (a^m)^n \ (b^n)^m = 1$, so the order of ab divides mn. Thus $|ab| = m_1 n_1$ where m_1 divides m and n_1 divides n. Consequently,

   $$a^{m_1 n_1} \ b^{m_1 n_1} = 1 \tag{1}$$

   If $m = m_1 m_2$, raise both sides of (1) to the power m_2 to get $b^{mn_1} = 1$. The order of b, namely n, must divide mn_1, and since m and n are relatively prime, n must divide n_1. But n_1 divides n, hence $n = n_1$. Similarly, if $n = n_1 n_2$ we raise both sides of (1) to the power n_2 and conclude as above that $m = m_1$. But then $|ab| = m_1 n_1 = mn$, as asserted.

If c belongs to both $\langle a \rangle$ and $\langle b \rangle$ then since c is a power of a and also a power of b, we have $c^m = c^n = 1$. But then the order of c divides both m and n, and since m and n are relatively prime, c has order 1, i.e., $c = 1$.

9. Let $|a| = m$, $|b| = n$. If $[m, n]$ is the least common multiple, and (m, n) the greatest common divisor, of m and n, then $[m, n] = mn/(m, n)$. Examine the prime factorizations of m and n:
$$m = (p_1^{t_1} \cdots p_i^{t_i})(p_{i+1}^{t_{i+1}} \cdots p_j^{t_j}) = r\ r'$$
$$n = (p_1^{u_1} \cdots p_i^{u_i})(p_{i+1}^{u_{i+1}} \cdots p_j^{u_j}) = s'\ s$$
where $t_k \leq u_k$ for $1 \leq k \leq i$, and $t_k \geq u_k$ for $i + 1 \leq k \leq j$.
Now a^r has order m/r and b^s has order n/s, with m/r $(= r')$ and n/s $(= s')$ relatively prime. By Problem 8, $a^r b^s$ has order $mn/rs = mn/(m, n) = [m, n]$. Thus given elements of orders m and n, we can construct another element whose order is the least common multiple of m and n. Since the least common multiple of m, n and q is $[[m, n], q]$, we can inductively find an element whose order is the least common multiple of the orders of all elements of G.

10. Choose an element a that belongs to H but not K, and an element b that belongs to K but not H, where H and K are subgroups whose union is G. Then ab must belong to either H or K, say $ab = h \in H$. But then $b = a^{-1}h \in H$, a contradiction. If $ab = k \in K$, then $a = kb^{-1} \in K$, again a contradiction. To prove the last statement, note that if $H \cup K$ is a subgroup, the first result with G replaced by $H \cup K$ implies that $H = H \cup K$ or $K = H \cup K$, in other words, $K \subseteq H$ or $H \subseteq K$.

11. $a^{km} = 1$ if and only if km is a multiple of n, and the smallest such multiple occurs when km is the least common multiple of n and k. Thus the order of a^k is $[n, k]/k$. Examination of the prime factorizations of n and k shows that $[n, k]/k = n/(n, k)$.

12. We have $x \in A_i$ iff x is a multiple of p_i, and there are exactly n/p_i multiples of p_i between 1 and n. Similarly, x belongs to $A_i \cap A_j$ iff x is divisible by $p_i p_j$, and there are exactly $\frac{n}{p_i p_j}$ multiples of $p_i p_j$ between 1 and n. The same technique works for all other terms.

13. The set of positive integers in $\{1, 2, \ldots, n\}$ and *not* relatively prime to n is $\cup_{i=1}^r A_i$, so $\varphi(n) = n - | \cup_{i=1}^r A_i|$. By the principle of inclusion and exclusion from basic combinatorics,
$$\Big|\bigcup_{i=1}^r A_i\Big| = \sum_{i=1}^r |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{r-1}|A_1 \cap A_2 \cap \cdots A_r|.$$
By Problem 12,
$$\varphi(n) = n\Big[1 - \sum_{i=1}^r \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_i p_j} - \sum_{i<j<k} \frac{1}{p_i p_j p_k} + \cdots + (-1)^r 1 p_1 p_2 \cdots p_r\Big].$$
Thus $\varphi(n) = n\big(1 - \frac{1}{p_1}\big)\big(1 - \frac{1}{p_2}\big) \cdots \big(1 - \frac{1}{p_r}\big)$.

14. Let G be cyclic of prime order p. Since the only positive divisors of p are 1 and p, the only subgroups of G are G and $\{1\}$.

15. No. Any non-identity element of G generates a cyclic subgroup H. If $H \subset G$, we are finished. If $H = G$, then G is isomorphic to the integers, and therefore has many nontrivial proper subgroups. (See (1.1.4) and Problem 6 above.)

Section 1.2

1. The cycle decomposition is $(1,4)(2,6,5)$; there is one cycle of even length, so the permutation is odd.
2. The elements are I, $R = (A,B,C,D)$, $R^2 = (A,C)(B,D)$, $R^3 = (A,D,C,B)$, $F = (B,D)$, $RF = (A,B)(C,D)$, $R^2F = (A,C)$, $R^3F = (A,D)(B,C)$.
3. Such a permutation can be written as $(1,a_1,a_2,a_3,a_4)$ where (a_1,a_2,a_3,a_4) is a permutation of $\{2,3,4,5\}$. Thus the number of permutations is $4! = 24$.
4. Select two symbols from 5, then two symbols from the remaining 3, and divide by 2 since, for example, $(1,4)(3,5)$ is the same as $(3,5)(1,4)$. The number of permutations is $10(3)/2 = 15$.
5. For example, $(1,2,3)(1,2) = (1,3)$ but $(1,2)(1,2,3) = (2,3)$.
6. We have $V = \{I,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$. Thus $V = \{I,a,b,c\}$ where the product of any two distinct elements from $\{a,b,c\}$ (in either order) is the third element, and the square of each element is I. It follows that V is an abelian group.
7. This follows because the inverse of the cycle $(a_1,a_2,\dots,a_k)$ is $(a_k,\dots,a_2,a_1)$.
8. Pick 3 symbols out of 4 to be moved, then pick one of two possible orientations, e.g., $(1,2,3)$ or $(1,3,2)$. The number of 3-cycles in S_4 is therefore $4(2) = 8$.
9. If π is a 3-cycle, then $\pi^3 = I$, so $\pi^4 = \pi$. But $\pi^4 = (\pi^2)^2$, and $\pi^2 \in H$ by hypothesis, so $(\pi^2)^2 \in H$ because H is a group. Thus $\pi \in H$.
10. There are 5 inversions, 21, 41, 51, 43 and 53. Thus we have an odd number of inversions and the permutation $\pi = (1,2,4)(3,5)$ is also odd.
11. This follows because a transposition of two adjacent symbols in the second row changes the number of inversions by exactly 1. Therefore such a transposition changes the parity of the number of inversions. Thus the parity of π coincides with the parity of the number of inversions. In the given example, it takes 5 transpositions of adjacent digits to bring 24513 into natural order 12345. It also takes 5 transpositions to create π:

$$\pi = (1,5)(1,4)(1,2)(3,5)(3,4)$$

Section 1.3

1. If $Ha = Hb$ then $a = 1a = hb$ for some $h \in H$, so $ab^{-1} = h \in H$. Conversely, if $ab^{-1} = h \in H$ then $Ha = Hhb = Hb$.
2. Reflexivity: $aa^{-1} = 1 \in H$.
   Symmetry: If $ab^{-1} \in H$ then $(ab^{-1})^{-1} = ba^{-1} \in H$.
   Transitivity: If $ab^{-1} \in H$ and $bc^{-1} \in H$ then $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$.
3. $ab^{-1} \in H$ iff $(ab^{-1})^{-1} = ba^{-1} \in H$ iff $b \in Ha$.
4. $Ha^{-1} = Hb^{-1}$ iff $a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$ iff $aH = bH$.
5. Since a_1 belongs to both aH and a_1H, we have $a_1H = aH$ because the left cosets partition G.

6. There are only two left cosets of H in G; one is H itself, and the other is, say, aH. Similarly, there are only two right cosets, H and Hb. Since the left cosets partition G, as do the right cosets, aH must coincide with Hb, so that every left coset if a right coset.
7. The permutations on the list are e, $(1,2,3)$, $(1,3,2)$, $(1,2)$, $(1,3)$, and $(2,3)$, which are in fact the 6 distinct permutations of $\{1,2,3\}$.
8. The left cosets of H are $H=\{e,b\}$, $aH=\{a,ab\}$, and $a^2H=\{a^2,a^2b\}$. The right cosets of H are $H=\{e,b\}$, $Ha=\{a,ba\}=\{a,a^2b\}$, and $Ha^2=\{a^2,ba^2\}=\{a^2,ab\}$.
9. The computation of Problem 8 shows that the left cosets of H do not coincide with the right cosets. Explicitly, aH and a^2H are not right cosets (and similarly, Ha and Ha^2 are not left cosets).
10. $f(n)=f(1+1+\cdots 1)=f(1)+f(1)+\cdots f(1)=r+r+\cdots r=rn$.
11. In Problem 10, the image $f(\mathbb{Z})$ must coincide with $\mathbb{Z}$. But $f(\mathbb{Z})$ consists of all multiples of r, and the only way $f(\mathbb{Z})$ can equal $\mathbb{Z}$ is for r to be ± 1.
12. The automorphism group of $\mathbb{Z}$ is $\{I,-I\}$ where $(-I)^2=I$. Thus the automorphisms of $\mathbb{Z}$ form a cyclic group of order 2. (There is only one such group, up to isomorphism.)
13. Reflexivity: $x=1x1$. Symmetry: If $x=hyk$, then $y=h^{-1}xk^{-1}$. Transitivity: if $x=h_1yk_1$ and $y=h_2zk_2$, then $x=h_1h_2zk_2k_1$.
14. HxK is the union over all $k\in K$ of the right cosets $H(xk)$, and also the union over all $h\in H$ of the left cosets $(hx)K$.

Section 1.4

1. Define $f\colon\mathbb{Z}\to\mathbb{Z}_n$ by $f(x)=$ the residue class of x mod n. Then f is an epimorphism with kernel $n\mathbb{Z}$, and the result follows from the first isomorphism theorem.
2. Define $f\colon\mathbb{Z}_n\to\mathbb{Z}_{n/m}$ by $f(x)=x \bmod n/m$. Then f is an epimorphism with kernel $\mathbb{Z}_m$, and the result follows from the first isomorphism theorem. (In the concrete example with $n=12$, $m=4$, we have $f(0)=0$, $f(1)=1$, $f(2)=2$, $f(3)=0$, $f(4)=1$, $f(5)=2$, $f(6)=0$, etc.)
3. $f(xy)=axya^{-1}=axa^{-1}aya^{-1}=f(x)f(y)$, so f is a homomorphism. If $b\in G$, we can solve $axa^{-1}=b$ for x, namely $x=a^{-1}ba$, so f is surjective. If $axa^{-1}=1$ then $ax=a$, so $x=1$ and f is injective. Thus f is an automorphism.
4. Note that $f_{ab}(x)=abx(ab)^{-1}=a(bxb^{-1})a^{-1}=f_a(f_b(x))$, and $y=f_a(x)$ iff $x=f_{a^{-1}}(y)$, so that $(f_a)^{-1}=f_{a^{-1}}$.
5. Define $\Psi\colon G\to \text{Inn } G$, the group of inner automorphisms of G, by $\Psi(a)=f_a$. Then $\Psi(ab)=f_{ab}=f_a\circ f_b=\Psi(a)\Psi(b)$, so Ψ is a homomorphism (see the solution to Problem 4). Since a is arbitrary, Ψ is surjective. Now a belongs to ker Ψ iff f_a is the identity function, i.e., $axa^{-1}=x$ for all $x\in G$, in other words, a commutes with every x in G. Thus ker $\Psi=Z(G)$, and the result follows from the first isomorphism theorem.
6. If f is an automorphism of $\mathbb{Z}_n$, then since 1 generates $\mathbb{Z}_n$, f is completely determined by $m=f(1)$, and since 1 has order n in $\mathbb{Z}_n$, m must have order n as well. But then m is a unit mod n (see (1.1.5)), and $f(r)=f(1+1+\cdots 1)=f(1)+f(1)+\cdots f(1)=rf(1)=$

rm. Conversely, any unit m mod n determines an automorphism $\theta(m) =$ multiplication by m. The correspondence between m and $\theta(m)$ is a group isomorphism because $\theta(m_1m_2) = \theta(m_1) \circ \theta(m_2)$.

7. The first assertion follows from the observation that HN is the subgroup generated by $H \cup N$ (see (1.3.6)). For the second assertion, note that if K is a subgroup of G contained in both H and N, then K is contained in $H \cap N$.
8. If $g(x) = y$, then $g \circ f_a \circ g^{-1}$ maps y to $g(axa^{-1}) = g(a)y[g(a)]^{-1}$.
9. If G is abelian, then $f_a(x) = axa^{-1} = aa^{-1}x = x$.

Section 1.5

1. $C_2 \times C_2$ has 4 elements $1 = (1,1)$, $\alpha = (a,1)$, $\beta = (1,a)$ and $\gamma = (a,a)$, and the product of any two distinct elements from $\{\alpha, \beta, \gamma\}$ is the third. Since each of α, β, γ has order 2 (and 1 has order 1), there is no element of order 4 and $C_2 \times C_2$ is not cyclic.
2. The four group is $V = \{I, a, b, c\}$ where the product of any two distinct elements from $\{a, b, c\}$ is the third. Therefore, the correspondence $1 \to I$, $\alpha \to a$, $\beta \to b$, $\gamma \to c$ is an isomorphism of $C_2 \times C_2$ and V.
3. Let $C_2 = \{1, a\}$ with $a^2 = 1$, and $C_3 = \{1, b, b^2\}$ with $b^3 = 1$. Then (a, b) generates $C_2 \times C_3$, since the successive powers of this element are (a, b), $(1, b^2)$, $(a, 1)$, $(1, b)$, (a, b^2), and $(1, 1)$. Therefore $C_2 \times C_3$ is cyclic of order 6, i.e., isomorphic to C_6.
4. Proceed as in Problem 3. If a has order n in C_n and b has order m in C_m, then (a, b) has order nm in $C_n \times C_m$, so that $C_n \times C_m$ is cyclic of order nm.
5. Suppose that (a, b) is a generator of the cyclic group $C_n \times C_m$. Then a must generate C_n and b must generate C_m (recall that $C_n \times \{1\}$ can be identified with C_n). But $(a, b)^k = 1$ iff $a^k = b^k = 1$, and it follows that the order of (a, b) is the least common multiple of the orders of a and b, i.e., the least common multiple of n and m. Since n and m are not relatively prime, the least common multiple is strictly smaller than nm, so that (a, b) cannot possibly generate $C_n \times C_m$, a contradiction.
6. By (1.3.3), G and H are both cyclic. Since p and q are distinct primes, they are relatively prime, and by Problem 4, $G \times H$ is cyclic.
7. Define $f\colon H \times K \to K \times H$ by $f(h, k) = (k, h)$. It follows from the definition of direct product that f is an isomorphism.
8. Define $f_1\colon G \times H \times K \to G \times (H \times K)$ by $f_1(g, h, k) = (g, (h, k))$, and define $f_2\colon G \times H \times K \to (G \times H) \times K$ by $f_2(g, h, k) = ((g, h), k)$. It follows from the definition of direct product that f_1 and f_2 are isomorphisms.

Section 2.1

1. Never. If f is a polynomial whose degree is at least 1, then f cannot have an inverse. For if $f(X)g(X) = 1$, then the leading coefficient of g would have to be 0, which is impossible.

2. If $f(X)g(X) = 1$, then (see Problem 1) f and g are polynomials of degree 0, in other words, elements of R. Thus the units of $R[X]$ are simply the nonzero elements of R.
3. (a) No element of the form $a_1X + a_2X^2 + \cdots$ can have an inverse.

   (b) For example, $1 - X$ is a unit because $(1 - X)(1 + X + X^2 + X^3 + \cdots) = 1$.
4. Since $\mathbb{Z}[i]$ is a subset of the field $\mathbb{C}$ of complex numbers, there can be no zero divisors in $\mathbb{Z}[i]$. If w is a nonzero Gaussian integer, then w has an inverse in $\mathbb{C}$, but the inverse need not belong to $\mathbb{Z}[i]$. For example, $(1 + i)^{-1} = \frac{1}{2} - \frac{1}{2}i$.
5. If $z = a + bi$ with a and b integers, then $|z|^2 = a^2 + b^2$, so that if z is not zero, we must have $|z| \geq 1$. Thus if $zw = 1$, so that $|z||w| = 1$, we have $|z| = 1$, and the only possibilities are $a = 0, b = \pm 1$ or $a = \pm 1, b = 0$. Consequently, the units of $\mathbb{Z}[i]$ are 1, -1, i and $-i$.
6. All identities follow directly from the definition of multiplication of quaternions. Alternatively, (b) can be deduced from (a) by interchanging x_1 and x_2, y_1 and y_2, z_1 and z_2, and w_1 and w_2. Then the second identity of (c) can be deduced by noting that the quaternion on the right side of the equals sign in (a) is the conjugate of the quaternion on the right side of the equals sign in (b).
7. Multiply identities (a) and (b), and use (c). (This is not how Euler discovered the identity; quaternions were not invented until much later.)
8. The verification that End G is an abelian group under addition uses the fact that G is an abelian group. The additive identity is the zero function, and the additive inverse of f is given by $(-f)(a) = -f(a)$. Multiplication is associative because composition of functions is associative. To establish the distributive laws, note that the value of $(f + g)h$ at the element $a \in G$ is $f(h(a)) + g(h(a))$, so that $(f + g)h = fh + gh$. Furthermore, the value of $f(g + h)$ at a is $f(g(a) + h(a)) = f(g(a)) + f(h(a))$ since f is an endomorphism. Therefore $f(g + h) = fh + gh$. The multiplicative identity is the identity function, given by $E(a) = a$ for all a.
9. An endomorphism that has an inverse must be an isomorphism of G with itself. Thus the units of the ring End G are the automorphisms of G.
10. Use Euler's identity with $x_1 = 1, y_1 = 2, z_1 = 2, w_1 = 5$ $(34 = 1^2 + 2^2 + 2^2 + 5^2)$ and $x_2 = 1, y_2 = 1, z_2 = 4, w_2 = 6$ $(54 = 1^2 + 1^2 + 4^2 + 6^2)$. The result is $1836 = (34)(54) = 41^2 + 9^2 + 5^2 + 7^2$. The decomposition is not unique; another possibility is $x_1 = 0, y_1 = 0, z_1 = 3, w_1 = 5, x_2 = 0, y_2 = 1, z_2 = 2, w_2 = 7$.
11. In all four cases, sums and products of matrices of the given type are also of that type. But in (b), there is no matrix of the given form that can serve as the multiplicative identity.. Thus the sets (a), (c) and (d) are rings, but (b) is not.

Section 2.2

1. By Section 1.1, Problem 6, the additive subgroups of $\mathbb{Z}$ are of the form $(n) =$ all multiples of n. But if $x \in (n)$ and $r \in \mathbb{Z}$ then $rx \in (n)$, so each (n) is an ideal as well.
2. If the n by n matrix A is 0 except perhaps in column k, and B is any n by n matrix, then BA is 0 except perhaps in column k. Similarly, if A is 0 off row k, then so is AB.

3. (a) This follows from the definition of matrix multiplication.

   (b) In (a) we have $a_{jr} = 0$ for $r \neq k$, and the result follows.

   (c) By (b), the i^{th} term of the sum is a matrix with c_{ik} in the ik position, and 0's elsewhere. The sum therefore coincides with C.

4. The statement about left ideals follows from the formula of Problem 3(c). The result for right ideals is proved in a similar fashion. Explicitly, AE_{ij} has column i of A as its j^{th} column, with 0's elsewhere. If $A \in R_k$ then AE_{ij} has a_{ki} in the kj position, with 0's elsewhere, so if $a_{ki} \neq 0$ we have $AE_{ij}a_{ki}^{-1} = E_{kj}$. Thus if $C \in R_k$ then

$$\sum_{j=1}^{n} AE_{ij}a_{ki}^{-1}c_{kj} = C.$$

5. If I is a two-sided ideal and $A \in I$ with $a_{rs} \neq 0$, then by considering products of the form $a_{rs}^{-1}E_{pq}AE_{kl}$ (which have the effect of selecting an entry of A and sliding it from one row or column to another), we can show that every matrix E_{ij} belongs to I. Since every matrix is a linear combination of the E_{ij}, it follows that $I = M_n(R)$.

6. A polynomial with no constant term is of the form $a_1X + a_2X^2 + \cdots a_nX^n = Xg(X)$. Conversely, a polynomial expressible as $Xg(X)$ has no constant term. Thus we may take $f = X$.

7. Let a be a nonzero element of R. Then the principal ideal (a) is not $\{0\}$, so $(a) = R$. Thus $1 \in (a)$, so there is an element $b \in R$ such that $ab = 1$.

8. Since an ideal I is a finite set in this case, it must have a finite set of generators $x_1, \dots, x_k$. Let d be the greatest common divisor of the x_i. Every element of I is of the form $a_1x_1 + \cdots + a_kx_k$, and hence is a multiple of d. Thus $I \subseteq (d)$. But $d \in I$, because there are integers a_i such that $\sum_i a_ix_i = d$. Consequently, $(d) \subseteq I$. [Technically, arithmetic is modulo n, but we get around this difficulty by noting that if $ab = c$ as integers, then $ab \equiv c$ modulo n.]

Section 2.3

1. Use the same maps as before, and apply the first isomorphism theorem for rings.

2. If I_n is the set of multiples of $n > 1$ in the ring of integers, then I_n is an ideal but not a subring (since $1 \notin I_n$). $\mathbb{Z}$ is a subring of the rational numbers $\mathbb{Q}$ but not an ideal, since a rational number times an integer need not be an integer.

3. In parts (2) and (3) of the Chinese remainder theorem, take $R = \mathbb{Z}$ and $I_i =$ the set of multiples of m_i.

4. Apply part (4) of the Chinese remainder theorem with $R = \mathbb{Z}$ and $I_i =$ the set of multiples of m_i.

5. To prove the first statement, define $f\colon R \to R_2$ by $f(r_1, r_2) = r_2$. Then f is a ring homomorphism with kernel R_1' and image R_2. By the first isomorphism theorem for rings, $R/R_1' \cong R_2$. A symmetrical argument proves the second statement. In practice, we tend to forget about the primes and write $R/R_1 \cong R_2$ and $R/R_2 \cong R_1$. There is

also a tendency to identify a ring with its isomorphic copy, and write $R/R_1 = R_2$ and $R/R_2 = R_1$ This should not cause any difficulty if you add, mentally at least, "up to isomorphism".

6. The product is always a subset of the intersection, by definition. First consider the case of two ideals. Then $1 = a_1 + a_2$ for some $a_1 \in I_1, a_2 \in I_2$. If $b \in I_1 \cap I_2$, then $b = b1 = ba_1 + ba_2 \in I_1I_2$. The case of more than two ideals is handled by induction. Note that $R = (I_1 + I_n)(I_2 + I_n) \cdots (I_{n-1} + I_n) \subseteq (I_1 \cdots I_{n-1}) + I_n$. Therefore $(I_1 \cdots I_{n-1}) + I_n = R$. By the $n = 2$ case and the induction hypothesis, $I_1 \cdots I_{n-1}I_n = (I_1 \cdots I_{n-1}) \cap I_n = I_1 \cap I_2 \cap \cdots \cap I_n$.
7. Let $a + \cap_i I_i$ map to $(1 + I_1, 0 + I_2, c_3 + I_3, \ldots, c_n + I_n)$, where the c_j are arbitrary. Then $1 - a \in I_1$ and $a \in I_2$, so $1 = (1 - a) + a \in I_1 + I_2$. Thus $I_1 + I_2 = R$, and similarly $I_i + I_j = R$ for all $i \neq j$.

Section 2.4

1. If $n = rs$ with $r, s > 1$ then $r \notin \langle n\rangle, s \notin \langle n\rangle$, but $rs \in \langle n\rangle$, so that $\langle n\rangle$ is not prime. But $\mathbb{Z}/\langle n\rangle$ is isomorphic to $\mathbb{Z}_n$, the ring of integers modulo n (see Section 2.3, Problem 1). If n is prime, then $\mathbb{Z}_n$ is a field, in particular an integral domain, hence $\langle n\rangle$ is a prime ideal by (2.4.5).
2. By Problem 1, I is of the form $\langle p\rangle$ where p is prime. Since $\mathbb{Z}/\langle p\rangle$ is isomorphic to $\mathbb{Z}_p$, which is a field, $\langle p\rangle$ is maximal by (2.4.3).
3. The epimorphism $a_0 + a_1X + a_2X^2 + \cdots \to a_0$ of $F[[X]]$ onto F has kernel $\langle X\rangle$, and the result follows from (2.4.7).
4. The ideal $I = \langle 2, X\rangle$ is not proper; since $2 \in I$ and $\frac{1}{2} \in F \subseteq F[[X]]$, we have $1 \in I$ and therefore $I = F[[X]]$. The key point is that F is a field, whereas $\mathbb{Z}$ is not.
5. Suppose that $f(X) = a_0 + a_1X + \cdots$ belongs to I but not to $\langle X\rangle$. Then a_0 cannot be 0, so by ordinary long division we can find $g(X) \in F[[X]]$ such that $f(X)g(X) = 1$. But then $1 \in I$, contradicting the assumption that I is proper.
6. Let $f(X) = a_nX^n + a_{n+1}X^{n+1} + \cdots, a_n \neq 0$, be an element of the ideal I, with n as small as possible. Then $f(X) \in (X^n)$, and if $g(X)$ is any element of I, we have $g(X) \in (X^m)$ for some $m \geq n$. Thus $I \subseteq (X^n)$. Conversely, if $f(X) = X^ng(X) \in I$, with $g(X) = a_n + a_{n+1}X + \cdots, a_n \neq 0,$, then as in Problem 5, $g(X)$ is a unit, and therefore $X^n \in I$. Thus $(X^n) \subseteq I$, so that $I = (X^n)$, as claimed.
7. $f^{-1}(P)$ is an additive subgroup by (1.3.15), part (ii). If $a \in f^{-1}(P)$ and $r \in R$, then $f(ra) = f(r)f(a) \in P$, so $ra \in f^{-1}(P)$. Thus $f^{-1}(P)$ is an ideal. If $ab \in f^{-1}(P)$, then $f(a)f(b) \in P$, so either a or b must belong to $f^{-1}(P)$. If $f^{-1}(P) = R$, then f maps eveything in R, including 1, into P; thus $f^{-1}(P)$ is proper. (Another method: As a proper ideal, P is the kernel of some ring homomorphism π. Consequently, $f^{-1}(P)$ is the kernel of $\pi \circ f$, which is also a ring homomorphism. Therefore $f^{-1}(P)$ is a proper ideal.) Consequently, $f^{-1}(P)$ is prime.
8. Let S be a field, and R an integral domain contained in S, and assume that R is not a field. For example, let $R = \mathbb{Z}$, $S = \mathbb{Q}$. Take f to be the inclusion map. Then $\{0\}$ is a maximal ideal of S, but $f^{-1}(\{0\}) = \{0\}$ is a prime but not maximal ideal of R.

9. If $P = I \cap J$ with $P \subset I$ and $P \subset J$, choose $a \in I \setminus P$ and $b \in J \setminus P$. Then $ab \in I \cap J = P$, contradicting the assumption that P is prime.

Section 2.5

1. Any number that divides a and b divides b and r_1, and conversely, any number that divides b and r_1 divides a and b. Iterating this argument, we find that $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{j-1}, r_j) = r_j$.
2. This follows by successive substitution. We start with $r_j = r_{j-2} - r_{j-1}q_j$, continue with $r_{j-1} = r_{j-3} - r_{j-2}q_{j-1}$, $r_{j-2} = r_{j-4} - r_{j-3}q_{j-2}$, and proceed up the ladder until we have expressed d as a linear combination of a and b. There is an easier way, as Problem 3 shows.
3. The first equation of the three describes the steps of the algorithm. We wish to prove that $ax_i + by_i = r_i$, that is,

$$a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) = r_i. \tag{1}$$

But this follows by induction: if $ax_{i-2} + by_{i-2} = r_{i-2}$ and $ax_{i-1} + by_{i-1} = r_{i-1}$, then the left side of (1) is $r_{i-2} - q_i r_{i-1}$, which is r_i by definition of the Euclidean algorithm.

4. We have the following table:

i	q_{i+1}	r_i	x_i	y_i
-1	—	123	1	0
0	2	54	0	1
1	3	15	1	-2
2	1	9	-3	7
3	1	6	4	-9
4	2	3	-7	16

For example, to go from $i = 1$ to $i = 2$ we have $x_2 = x_0 - q_2 x_1 = 0 - 3(1) = -3$, $y_2 = y_0 - q_2 y_1 = 1 - 3(-2) = 7$, and $r_2 = r_0 - q_2 r_1 = 54 - 3(15) = 9$; also, $q_3 = \lfloor 15/9 \rfloor = 1$. We have $ax_2 + by_2 = 123(-3) + 54(7) = 9 = r_2$, as expected. The process terminates with $123(-7) + 54(16) = 3 = d$.

5. If p is composite, say $p = rs$ with $1 < r < p$, $1 < s < p$, then rs is 0 in $\mathbb{Z}_p$ but r and s are nonzero, so $\mathbb{Z}_p$ is not a field. If p is prime and a is not zero in $\mathbb{Z}_p$ then the greatest common divisor of a and p is 1, and consequently there are integers x and y such that $ax + py = 1$. In $\mathbb{Z}_p$ this becomes $ax = 1$, so that every nonzero element in $\mathbb{Z}_p$ has an inverse in $\mathbb{Z}_p$, proving that $\mathbb{Z}_p$ is a field.
6. Since $f(X)$ and $g(X)$ are multiples of $d(X)$, so are all linear combinations $a(X)f(X) + b(X)g(X)$, and consequently $I \subseteq J$. By Problem 2, there are polynomials $a(X)$ and $b(X)$ such that $a(X)f(X) + b(X)g(X) = d(X)$, so that $d(X)$ belongs to I. Since I is an ideal, every multiple of $d(X)$ belongs to I, and therefore $J \subseteq I$.
7. Take $f(X) = \sum_{i=0}^{n} b_i P_i(X)$.

8. If $g(X)$ is another polynomial such that $g(a_i) = f(a_i)$ for all i, then f and g agree at $n+1$ points, so that $f(X)-g(X)$ has more than n roots in F. By (2.5.3), $f(X)-g(X)$ must be the zero polynomial.
9. If F has only finitely many elements $a_1, \dots, a_n$, take $f(X) = (X - a_1) \cdots (X - a_n)$.
10. Let F be the complex numbers $\mathbb{C}$. Then every polynomial of degree n has exactly n roots, counting multiplicity. Thus if $f(a) = 0$ at more than n points a, in particular if f vanishes at every point of $\mathbb{C}$, then $f = 0$. More generally, F can be any infinite field (use (2.5.3)).

Section 2.6

1. If $r = 0$ then I contains a unit, so that $1 \in I$ and $I = R$.
2. If $b \notin \langle p_1 \rangle$ then $b + \langle p_1 \rangle \neq \langle p_1 \rangle$, so $b + \langle p_1 \rangle$ has an inverse in $R/\langle p_1 \rangle$, say $c + \langle p_1 \rangle$. Thus $(b + \langle p_1 \rangle)(c + \langle p_1 \rangle) = 1 + \langle p_1 \rangle$, hence $(bc - 1) + \langle p_1 \rangle = \langle p_1 \rangle$, so $bc - 1 \in \langle p_1 \rangle$.
3. If $bc - dp_1 = 1$ then $bcp_2 \cdots p_n - dp_1 \cdots p_n = p_2 \cdots p_n$, and since b and $p_1 \cdots p_n$ belong to I, so does $p_2 \cdots p_n$, contradicting the minimality of n. (If $n = 1$, then $1 \in I$, so $I = R$.)
4. If $a, b \in R$ and $x, y \in J$ then $(ax + by)p_1 = xp_1a + yp_1b$. Since $x, y \in J$ we have $xp_1 \in I$ and $yp_1 \in I$, so that $(ax + by)p_1 \in I$, hence $ax + by \in J$.
5. If $x \in J$ then $xp_1 \in I$, so $Jp_1 \subseteq I$. Now $I \subseteq \langle p_1 \rangle$ by Problem 3, so if $a \in I$ then $a = xp_1$ for some $x \in R$. But then $x \in J$ by definition of J, so $a = xp_1 \in Jp_1$.
6. Since J contains a product of fewer than n primes, J is principal by the induction hypothesis. If $J = \langle d \rangle$ then by Problem 5, $I = J\langle p_1 \rangle$. But then $I = \langle dp_1 \rangle$, and the result follows. (If $n = 1$, then $p_1 \in I$, hence $1 \in J$, so $J = R$ and $I = J\langle p_1 \rangle = \langle p_1 \rangle$.)
7. Assume that $P \subseteq Q$. Then $p = aq$ for some $a \in R$, so $aq \in P$. Since P is prime, either a or q belongs to P. In the second case, $Q \subseteq P$ and we are finished. Thus assume $a \in P$, so that $a = bp$ for some $b \in R$. Then $p = aq = bpq$, and since R is an integral domain and $p \neq 0$, we have $bq = 1$, so q is a unit and $Q = R$, a contradiction of the assumption that Q is prime.
8. Let x be a nonzero element of P, with $x = up_1 \cdots p_n$, u a unit and the p_i prime. Then $p_1 \cdots p_n = u^{-1}x \in P$, and since P is prime, some p_i belongs to P. Thus P contains the nonzero principal prime ideal $\langle p_i \rangle$.

Section 2.7

1. If m is a generator of the indicated ideal then m belongs to all $\langle a_i \rangle$, so each a_i divides m. If each a_i divides b then b is in every $\langle a_i \rangle$, so $b \in \cap_{i=1}^n \langle a_i \rangle = \langle m \rangle$, so m divides b. Thus m is a least common multiple of A. Now suppose that m is an lcm of A, and let $\cap_{i=1}^n \langle a_i \rangle = \langle c \rangle$. Then c belongs to every $\langle a_i \rangle$, so each a_i divides c. Since $m = \operatorname{lcm}(A)$, m divides c, so $\langle c \rangle$ is a subset of $\langle m \rangle$. But again since $m = \operatorname{lcm}(A)$, each a_i divides m, so $m \in \cap_{i=1}^n \langle a_i \rangle = \langle c \rangle$. Therefore $\langle m \rangle \subseteq \langle c \rangle$, hence $\langle m \rangle = \langle c \rangle$, and m is a generator of $\cap_{i=1}^n \langle a_i \rangle$.

2. Let $a = 11 + 3i$, $b = 8 - i$. Then $a/b = (11 + 3i)(8 + i)/65 = 85/65 + i35/65$. Thus we may take $x_0 = y_0 = 1$, and the first quotient is $q_1 = 1 + i$. The first remainder is $r_1 = a - bq_1 = (11 + 3i) - (8 - i)(1 + i) = 2 - 4i$. The next step in the Euclidean algorithm is $(8-i)/(2-4i) = (8-i)(2+4i)/20 = 1+(3i/2)$. Thus the second quotient is $q_2 = 1 + i$ ($q_2 = 1 + 2i$ would be equally good). The second remainder is $r_2 = (8-i)-(2-4i)(1+i) = 2+i$. The next step is $(2-4i)/(2+i) = (2-4i)(2-i)/5 = -2i$, so $q_3 = -2i$, $r_3 = 0$. The gcd is the last divisor, namely $2 + i$.
3. We have $\Psi(1) \leq \Psi(1(a)) = \Psi(a)$ for every nonzero a. If a is a unit with $ab = 1$, then $\Psi(a) \leq \Psi(ab) = \Psi(1)$, so $\Psi(a) = \Psi(1)$. Conversely, suppose that $a \neq 0$ and $\Psi(a) = \Psi(1)$. Divide 1 by a to get $1 = aq + r$, where $r = 0$ or $\Psi(r) < \Psi(a) = \Psi(1)$. But if $r \neq 0$ then $\Psi(r)$ must be greater than or equal to $\Psi(1)$, so we must have $r = 0$. Therefore $1 = aq$, and a is a unit.
4. $$\begin{aligned}&\Psi((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}))\\ &\qquad= \psi(a_1a_2 + b_1b_2d + (a_1b_2 + a_2b_1)\sqrt{d})\\ &\qquad= \big|a_1a_2 + b_1b_2d + (a_1b_2 + a_2b_1)\sqrt{d}\big|\big|a_1a_2 + b_1b_2d - (a_1b_2 + a_2b_1)\sqrt{d}\big|;\\ &\Psi(a_1 + b_1\sqrt{d})\Psi(a_2 + b_2\sqrt{d})\\ &\qquad= \big|a_1 + b_1\sqrt{d}\big|\big|a_2 + b_2\sqrt{d}\big|\big|a_1 - b_1\sqrt{d}\big|\big|a_2 - b_2\sqrt{d}\big|\end{aligned}$$
   and it follows that $\Psi(\alpha\beta) = \Psi(\alpha)\Psi(\beta)$. Now $\Psi(\alpha) \geq 1$ for all nonzero α, for if $\Psi(\alpha) = |a^2 - db^2| = 0$, then $a^2 = db^2$. But if $b \neq 0$ then $d = (a/b)^2$, contradicting the assumption that d is not a perfect square. Thus $b = 0$, so a is 0 as well, and $\alpha = 0$, a contradiction. Thus $\Psi(\alpha\beta) = \Psi(\alpha)\Psi(\beta) \geq \Psi(\alpha)$.
5. Either d or $d - 1$ is even, so 2 divides $d(d - 1) = d^2 - d = (d + \sqrt{d})(d - \sqrt{d})$. But 2 does not divide $d + \sqrt{d}$ or $d - \sqrt{d}$. For example, if $2(a + b\sqrt{d}) = d + \sqrt{d})$ for integers a, b then $2a - d = (1 - 2b)\sqrt{d}$, which is impossible since $\sqrt{d}$ is irrational. (If $\sqrt{d} = r/s$ then $r^2 = ds^2$, which cannot happen if d is not a perfect square.)
6. Define Ψ as in Problem 4 (and Example (2.7.5)). Suppose $2 = \alpha\beta$ where α and β are nonunits in $\mathbb{Z}[\sqrt{d}]$. Then $4 = \Psi(2) = \Psi(\alpha)\Psi(\beta)$, with $\Psi(\alpha)$, $\Psi(\beta) > 1$ by Problems 3 and 4. But then $\Psi(\alpha) = \Psi(\beta) = 2$. If $\alpha = a + b\sqrt{d}$ then $|a^2 - db^2| = 2$, so $a^2 - db^2$ is either 2 or -2. Therefore if $b \neq 0$ (so that $b^2 \geq 1$), then since $d \leq -3$ we have
   $$a^2 - db^2 \geq 0 + 3(1) = 3,$$
   a contradiction. Thus $b = 0$, so $\alpha = a$, and $2 = \Psi(a) = a^2$, an impossibility for $a \in \mathbb{Z}$.
7. This follows from Problems 5 and 6, along with (2.6.4).
8. Just as with ordinary integers, the product of two Gaussian integers is their greatest common divisor times their least common multiple. Thus by Problem 2, the lcm is $(11 + 3i)(8 - i)/(2 + i) = 39 - 13i$.
9. If $\alpha = \beta\gamma$, then $\Psi(\alpha) = \Psi(\beta)\Psi(\gamma)$. By hypothesis, either $\Psi(\beta)$ or $\Psi(\gamma)$ is $1(= \Psi(1))$. By Problem 3, either β or γ is a unit.

Section 2.8

1. If D is a field, then the quotient field F, which can be viewed as the smallest field containing D, is D itself. Strictly speaking, F is isomorphic to D; the embedding map

$f(a) = a/1$ is surjective, hence an isomorphism. To see this, note that if $a/b \in F$, then $a/b = ab^{-1}/1 = f(ab^{-1})$.

2. The quotient field consists of all rational functions $f(X)/g(X)$, where $f(X)$ and $g(X)$ are polynomials in $F[X]$ and $g(X)$ is not the zero polynomial. To see this, note that the collection of rational functions is in fact a field, and any field containing $F[X]$ must contain all such rational functions.
3. $\dfrac{a}{b} + \left(\dfrac{c}{d} + \dfrac{e}{f}\right)$ and $\left(\dfrac{a}{b} + \dfrac{c}{d}\right) + \dfrac{e}{f}$ both compute to be $\dfrac{adf + bcf + bde}{bdf}$.
4. $\dfrac{a}{b}\left(\dfrac{c}{d} + \dfrac{e}{f}\right) = \dfrac{a}{b}\left(\dfrac{cf + de}{df}\right) = \dfrac{acf + ade}{bdf}$ and

   $\dfrac{ac}{bd} + \dfrac{ae}{bf} = \dfrac{acbf + bdae}{b^2df} = \dfrac{acf + dae}{bdf} = \dfrac{acf + ade}{bdf}$.
5. If g is any extension of h and $a/b \in F$, there is only one possible choice for $g(a/b)$, namely $h(a)/h(b)$. (Since $b \neq 0$ and h is a monomorphism, $h(b) \neq 0$.) If we define g this way, then $g(a) = g(a/1) = h(a)/h(1) = h(a)$, so g is in fact an extension of f. Furthermore, if $a/b = c/d$ then since h is a monomorphism, $h(a)/h(b) = h(c)/h(d)$. Therefore g is well-defined. Again since h is a monomorphism, it follows that $g\big(\frac{a}{b} + \frac{c}{d}\big) = g\big(\frac{a}{b}\big) + g\big(\frac{c}{d}\big)$ and $g\big(\frac{a}{b}\frac{c}{d}\big) = g\big(\frac{a}{b}\big)g\big(\frac{c}{d}\big)$. Since g is an extension of h, we have $g(1) = 1$, so g is a homomorphism. Finally, if $g(a/b) = 0$, then $h(a) = 0$, so $a = 0$ by injectivity of h. Thus g is a monomorphism.
6. The problem is that h is not injective. As before, if g is to be an extension of h, we must have $g(a/b) = h(a)/h(b)$. But if b is a multiple of p, then $h(b)$ is zero, so no such g can exist.
7. We must have $\overline{g}(a/b) = \overline{g}(a/1)\overline{g}((b/1)^{-1}) = g(a)g(b)^{-1}$.
8. If $a/b = c/d$, then for some $s \in S$ we have $s(ad - bc) = 0$. So $g(s)[g(a)g(d) - g(b)g(c)] = 0$. Since $g(s)$ is a unit, we may multiply by its inverse to get $g(a)g(d) = g(b)g(c)$, hence $g(a)g(b)^{-1} = g(c)g(d)^{-1}$, proving that $\overline{g}$ is well-defined. To show that $\overline{g}$ is a homomorphism, we compute

$$\begin{aligned}\overline{g}\left(\frac{a}{b} + \frac{c}{d}\right) &= \overline{g}\left(\frac{ad + bc}{bd}\right) = g(ad + bc)g(bd)^{-1} \\ &= [g(a)g(d) + g(b)g(c)]g(b)^{-1}g(d)^{-1} = \overline{g}\left(\frac{a}{b}\right) + \overline{g}\left(\frac{c}{d}\right)\end{aligned}$$

   Similarly, we have $\overline{g}\big(\frac{a}{b}\frac{c}{d}\big) = \overline{g}\big(\frac{a}{b}\big)\overline{g}\big(\frac{c}{d}\big)$ and $\overline{g}(1) = 1$.

Section 2.9

1. We have $a_n(u/v)^n + a_{n-1}(u/v)^{n-1} + \cdots + a_1(u/v) + a_0 = 0$; multiply by v^n to get

$$a_nu^n + a_{n-1}u^{n-1}v + \cdots + a_1uv^{n-1} + a_0v^n = 0.$$

   Therefore

$$a_nu^n = -a_{n-1}u^{n-1}v - \cdots - a_1uv^{n-1} - a_0v^n.$$

Since v divides the right side of this equation, it must divide the left side as well, and since u and v are relatively prime, v must divide a_n. Similarly,

$$a_0v^n = -a_nu^n - a_{n-1}u^{n-1}v - \cdots - a_1uv^{n-1},$$

so u divides a_0.

2. $X^n - p$ satisfies Eisenstein's criterion, and since the polynomial is primitive, it is irreducible over $\mathbb{Z}$.
3. $f_3(X) = X^3+2X+1$, which is irreducible over $\mathbb{Z}_3$. For if $f_3(X)$ were reducible over $\mathbb{Z}_3$, it would have a linear factor (since it is a cubic), necessarily $X-1$ or $X+1(=X-2)$. But then 1 or 2 would be a root of f_3, a contradiction since $f_3(1) = 1$ and $f_3(2) = 1 \pmod 3$.
4. By Eisenstein, $X^4 + 3$ is irreducible over $\mathbb{Z}$. The substitution $X = Y + 1$ yields $Y^4 + 4Y^3 + 6Y^2 + 4Y + 4$, which is therefore irreducible in $\mathbb{Z}[Y]$. Thus $X^4 + 4X^3 + 6X^2 + 4X + 4$ is irreducible in $\mathbb{Z}[X]$, i.e., irreducible over $\mathbb{Z}$.
5. Note that $\langle n, X\rangle$ is a proper ideal since it cannot contain 1. If $\langle n, X\rangle = \langle f\rangle$ then $n \in \langle f\rangle$, so n is a multiple of f. Thus f is constant ($\neq 1$), in which case $X \notin \langle f\rangle$.
6. Since $1 \notin \langle X, Y\rangle$, $\langle X, Y\rangle$ is a proper ideal. Suppose $\langle X, Y\rangle = \langle f\rangle$. Then Y is a multiple of f, so f is a polynomial in Y alone (in fact $f = cY$). But then $X \notin \langle f\rangle$, a contradiction.
7. If $p = X + i$, then p is irreducible since $X + i$ is of degree 1. Furthermore, p divides $X^2 + 1$ but p^2 does not. Take the ring R to be $\mathbb{C}[X, Y] = (\mathbb{C}[X])[Y]$ and apply Eisenstein's criterion.
8. Write $f(X, Y)$ as $Y^3+(X^3+1)$ and take $p = X+1$. Since $X^3+1 = (X+1)(X^2-X+1)$ and $X + 1$ does not divide $X^2 - X + 1$, the result follows as in Problem 7.

Section 3.1

1. $F(S)$ consists of all quotients of finite linear combinations (with coefficients in F) of finite products of elements of S. To prove this, note first that the set A of all such quotients is a field. Then observe that any field containing F and S must contain A, in particular, $A \subseteq F(S)$. But $F(S)$ is the smallest subfield containing F and S, so $F(S) \subseteq A$.
2. The composite consists of all quotients of finite sums of products of the form $x_{i_1}x_{i_2}\cdots x_{i_n}$, $n = 1, 2, \dots$, where $i_1, i_2, \dots, i_n \in I$ and $x_{i_j} \in K_{i_j}$. As in Problem 1, the set A of all such quotients is a field, and any field that contains all the K_i must contain A.
3. By (3.1.9), $[F[\alpha] : F] = [F[\alpha] : F[\beta]][F[\beta] : F]$, and since the degree of any extension is at least 1, the result follows.
4. Let $\min(-1+\sqrt{2}, \mathbb{Q}) = a_0+a_1X+X^2$ (a polynomial of degree 1 cannot work because $-1 + \sqrt{2} \notin \mathbb{Q}$). Then $a_0 + a_1(-1 + \sqrt{2}) + (-1 + \sqrt{2})^2 = 0$. Since $(-1 + \sqrt{2})^2 = 3 - 2\sqrt{2}$, we have $a_0 - a_1 + 3 = 0$ and $a_1 - 2 = 0$, so $a_0 = -1, a_1 = 2$. Therefore $\min(-1 + 2\sqrt{2}, \mathbb{Q}) = X^2 + 2X - 1$.

5. Let $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$. Then for some $a_0, \dots, a_n \in F$ we have $a_0 + a_1\beta + \cdots + a_n\beta^n = 0$. Substituting the expression for β in terms of α into this equation, reducing to a polynomial in α of degree at most $n-1$ (as in the proof of (3.1.7)), and setting the coefficients of the α^i, $i = 0, 1, \dots, n-1$ equal to zero (remember that the α^i form a basis for $F[\alpha]$ over F), we get n linear equations in the $n+1$ unknowns a_i, $i = 0, \dots, n$. We know that a solution exists because β is algebraic over F. By brute force (try $a_i = 1$, $a_j = 0$, $j > i$ for $i = 1, 2, \dots, n$), we will eventually arrive at the minimal polynomial.
6. Define $\varphi\colon F(X) \to E$ by $\varphi(f(X)/g(X)) = f(\alpha)/g(\alpha)$. Note that φ is well-defined, since if g is a nonzero polynomial, then $g(\alpha) \neq 0$ (because α is transcendental over F). By (3.1.2), φ is a monomorphism. Since $\varphi(F(X)) = F(\alpha)$, it follows that $F(X)$ and $F(\alpha)$ are isomorphic.
7. The kernel of φ is I, and as in (3.1.3), $F[X]/I$ is a field. The image of φ is $F[\alpha]$, and by the first isomorphism theorem for rings, $F[\alpha]$ is isomorphic to $F[X]/I$. Therefore $F[\alpha]$ is a field, and consequently $F[\alpha] = F(\alpha)$.
8. If $f = gh$, then $(g+I)(h+I) = 0$ in $F[X]/I$, so $F[X]/I$ is not a field. By (2.4.3), I is not maximal.
9. The minimal polynomial over F belongs to $F[X] \subseteq E[X]$, and has α as a root. Thus $\min(\alpha, E)$ divides $\min(\alpha, F)$.
10. The result is true for $n = 1$; see (3.1.7). Let $E = F[\alpha_1, \dots, \alpha_{n-1}]$, so that $[F[\alpha_1, \dots, \alpha_n] : F] = [F[\alpha_1, \dots, \alpha_n] : E][E : F] = [E[\alpha_n] : E][E : F]$. But $[E[\alpha_n] : E]$ is the degree of the minimal polynomial of α_n over E, which is at most the degree of the minimal polynomial of α_n over F, by Problem 9. An application of the induction hypothesis completes the proof.

Section 3.2

1. $f(X) = (X-2)^2$, so we may take the splitting field K to be Q itself.
2. $f(X) = (X-1)^2 + 3$, with roots $1 \pm i\sqrt{3}$, so $K = \mathbb{Q}(i\sqrt{3})$. Now $i\sqrt{3} \notin \mathbb{Q}$ since $(i\sqrt{3})^2 = -3 < 0$, so $[K : \mathbb{Q}] \geq 2$. But $i\sqrt{3}$ is a root of $X^2 + 3$, so $[K : \mathbb{Q}] \leq 2$. Therefore $[K : \mathbb{Q}] = 2$.
3. Let α be the positive 4^{th} root of 2. The roots of $f(X)$ are $\alpha, i\alpha, -\alpha$ and $-i\alpha$. Thus $K = \mathbb{Q}(\alpha, i)$. Now $f(X)$ is irreducible by Eisenstein, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Since $i \notin \mathbb{Q}(\alpha)$ and i is a root of $X^2 + 1 \in \mathbb{Q}(\alpha)[X]$, we have $[K : \mathbb{Q}(\alpha)] = 2$. By (3.1.9), $[K : \mathbb{Q}] = 2 \times 4 = 8$.
4. The argument of (3.2.1) may be reproduced, with the polynomial f replaced by the family $\mathcal{C}$ of polynomials, and the roots $\alpha_1, \dots, \alpha_k$ of f by the collection of all roots of the polynomials in the family $\mathcal{C}$.
5. Take $f = f_1 \cdots f_r$. Since α is a root of f iff α is a root of some f_i, the result follows.
6. If the degree is less than 4, it must be 2 (since $\sqrt{m} \notin \mathbb{Q}$). In this case, $\sqrt{n} = a + b\sqrt{m}$, so $n = a^2 + b^2m + 2ab\sqrt{m}$. Since m is square-free, we must have $a = 0$ or $b = 0$, and the latter is impossible because n is square-free. Thus $\sqrt{n} = b\sqrt{m}$, so $n = b^2m$, a contradiction of the hypothesis that m and n are distinct and square-free.

Section 3.3

1. If $\alpha_1, \dots, \alpha_n$ form a basis for E over F, then E is generated over F by the α_i. Each α_i is algebraic over F because $F(\alpha_i) \subseteq E$, and (3.1.10) applies.
2. There are only countably many polynomials with rational coefficients, and each such polynomial has only finitely many roots. Since an algebraic number must be a root of one of these polynomials, the set of algebraic numbers is countable. Since the complex field is uncountably infinite, there are uncountably many transcendental numbers.
3. The complex field $\mathbb{C}$ is algebraically closed, and $\mathbb{C}$ is an extension of the rational field $\mathbb{Q}$. But $\mathbb{C}$ is not algebraic over $\mathbb{Q}$, by Problem 2.
4. The algebraic numbers A form a field by (3.3.4), and A is algebraic over $\mathbb{Q}$ by definition. But it follows from Section 2.9, Problem 2, that A contains subfields of arbitrarily high degree (in fact subfields of every degree) over $\mathbb{Q}$, so that $A/\mathbb{Q}$ is not finite.
5. This can be verified by transfinite induction. A splitting field is always an algebraic extension (see (3.2.2)), and the field $F_{<f}$ is algebraic over F by the induction hypothesis. The result follows from (3.3.5).
6. By definition of algebraic number, A is an algebraic extension of $\mathbb{Q}$. If α is algebraic over A, then as in (3.3.5), α is algebraic over $\mathbb{Q}$, so $\alpha \in A$. Thus A has no proper algebraic extensions, so by (3.3.1), A is algebraically closed.
7. Since E is an extension of F we have $|F| \le |E|$. Suppose that $\alpha \in E$ and the minimal polynomial f of α has roots $\alpha_1, \dots, \alpha_n$, with $\alpha = \alpha_i$. Then the map $\alpha \to (f, i)$ is injective, since f and i determine α. It follows that $|E| \le |F[X]|\aleph_0 = |F[X]|$. But for each n, the set of polynomials of degree n over F has cardinality $|F|^{n+1} = |F|$, so $|F[X]| = |F|\aleph_0 = |F|$. Thus $|E| = |F|$.
8. Let C be an algebraic closure of F, and let A be the set of roots in C of all polynomials in S. Then $F(A)$, the field generated over F by the elements of A, is a splitting field for S over F; see Section 3.2, Problem 4.
9. If F is a finite field with elements $a_1, \dots, a_n$, the polynomial $f(X) = 1 + \prod_{i=1}^{n}(X - a_i)$ has no root in F, so F cannot be algebraically closed.

Section 3.4

1. Let $f(X) = (X - 1)^p$ over $\mathbb{F}_p$.
2. α is a root of $X^p - \alpha^p = (X - \alpha)^p$, so $m(X)$ divides $(X - \alpha)^p$.
3. By Problem 2, $m(X) = (X - \alpha)^r$ for some r. We are assuming that α is separable over $F(\alpha^p)$, so $m(X)$ must be simply $X - \alpha$. But then $\alpha \in F(\alpha^p)$.
4. The "if" part follows from the proof of (3.4.5), so assume that F is perfect and let $b \in F$. Let $f(X) = X^p - b$ and adjoin a root α of f. Then $\alpha^p = b$, so $F(\alpha^p) = F(b) = F$. By hypothesis, α is separable over $F = F(\alpha^p)$, so by Problem 3, $\alpha \in F$. But then b is the p^{th}power of an element of F.
5. If $\alpha_1, \dots, \alpha_n$ is a basis for E over F, then by the binomial expansion mod p, $K = F(\alpha_1^p, \dots, \alpha_n^p)$. Now since E/F is algebraic, the elements of $F(\alpha_1^p)$ can be expressed as polynomials in α_1^p with coefficients in F. Continuing, α_2^p is algebraic over

F, hence over $F(\alpha_1^p)$, so each element of $F(\alpha_1^p, \alpha_2^p)$ can be written as a polynomial in α_2^p with coefficients in $F(\alpha_1^p)$. Such an element has the form

$$\sum_s \Big(\sum_r b_{rs}\alpha_1^{pr}\Big)\alpha_2^{ps}$$

with the $b_{rs} \in F$. An induction argument completes the proof.

6. Extend the y_i to a basis $y_1, \dots, y_n$ for E over F. By Problem 5, every element of $E(= F(E^p))$ has the form $y = a_1 y_1^p + \cdots + a_n y_n^p$ with the $a_i \in F$. Thus $\{y_1^p, \dots, y_n^p\}$ spans E over F. It follows that this set contains a basis, hence (since there are exactly n vectors in the set) the set *is* a basis for E over F. The result follows.
7. Assume the extension is separable, and let $\alpha \in E$. Then α is separable over F, hence over $F(\alpha^p)$, so by Problem 3, $\alpha \in F(E^p)$. Thus $E = F(E^p)$. Conversely, suppose that $E = F(E^p)$ and the element $\alpha \in E$ has an inseparable minimal polynomial $m(X)$. By (3.4.3), $m(X)$ is of the form $b_0 + b_1 X^p + \cdots + b_{r-1}X^{(r-1)p} + X^{rp}$. Since $m(\alpha) = 0$, the elements $1, \alpha^p, \dots, \alpha^{rp}$ are linearly dependent over F. But by minimality of $m(X)$, $1, \alpha, \dots, \alpha^{rp-1}$ are linearly independent over F, hence $1, \alpha, \dots, \alpha^r$ are linearly independent over F. (Note that $rp - 1 \geq 2r - 1 \geq r$.) By Problem 6, $1, \alpha^p, \dots, \alpha^{rp}$ are linearly independent over F, which is a contradiction. Thus E/F is separable.
8. We may assume that F has prime characteristic p. By Problem 7, $E = K(E^p)$ and $K = F(K^p)$. Thus $E = F(K^p, E^p) = F(E^p)$ since $K \leq E$. Again by Problem 7, E/F is separable.
9. If g can be factored, so can f , and therefore g is irreducible. If $f(X) = g(X^{p^m})$ with m maximal, then $g \notin F[X^p]$. By (3.4.3) part (2), g is separable.
10. Suppose that the roots of g in a splitting field are $c_1, \dots, c_r$. Then $f(X) = g(X^{p^m}) = (X^{p^m} - c_1)\cdots(X^{p^m} - c_r)$. By separability of g, the c_j must be distinct, and since $f(\alpha) = 0$, we have $\alpha^{p^m} = c_j$ for all j. This is impossible unless $r = 1$, in which case $f(X) = X^{p^m} - c_1$. But $f \in F[X]$, so $\alpha^{p^m} = c_1 \in F$.
11. If $\alpha^{p^n} = c \in F$, then α is a root of $X^{p^n} - c = (X - \alpha)^{p^n}$, so $\min(\alpha, F)$ is a power of $X - \alpha$, and therefore has only one distinct root α. The converse follows from Problem 10 with $f = \min(\alpha, F)$.

Section 3.5

1. Take $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ (see (3.5.3)), and let E be any extension of K that is normal over F, for example, $E = \mathbb{C}$.
2. The polynomial $f(X) = X^2 - a$ is irreducible, else it would factor as $(X - b)(X - c)$ with $b + c = 0$, $bc = a$, i.e., $(X - b)(X + b)$ with $b^2 = a$, contradicting the hypothesis. Thus E is obtained from $\mathbb{Q}$ by adjoining a root of f. The other root of f is $-\sqrt{a}$, so that E is a splitting field of f over $\mathbb{Q}$. By (3.5.7), $E/\mathbb{Q}$ is normal.
3. Take $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $E = \mathbb{Q}(\sqrt[4]{2})$. Then K/F is normal by Problem 2, and E/K is normal by a similar argument. But E/F is not normal, since the two complex roots of $X^4 - 2$ do not belong to E. The same argument works with 2 replaced by any positive integer that is not a perfect square.

4. There are *at most* n embeddings of E in C extending σ. The proof is the same, except that now g has at most r distinct roots in C, so there are at most r possible choices of β. The induction hypothesis yields at most n/r extensions from $F(\alpha)$ to E, and the result follows.
5. Since the rationals have characteristic zero, the extension is separable. Since E is the splitting field of $(X^2-2)(X^2-3)$ over $\mathbb{Q}$, the extension is normal, hence Galois.
6. Since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, the extension has degree 4. By (3.5.9), there are exactly four $\mathbb{Q}$-automorphisms in the Galois group. By (3.5.1), each such $\mathbb{Q}$-automorphism must permute the roots of X^2-2 and must also permute the roots of X^2-3. There are only four possible ways this can be done. Since a $\mathbb{Q}$-automorphism is completely specified by its action on $\sqrt{2}$ and $\sqrt{3}$, the Galois group may be described as follows:

   (1) $\sqrt{2} \to \sqrt{2}, \qquad \sqrt{3} \to \sqrt{3};$

   (2) $\sqrt{2} \to \sqrt{2}, \qquad \sqrt{3} \to -\sqrt{3};$

   (3) $\sqrt{2} \to -\sqrt{2}, \qquad \sqrt{3} \to \sqrt{3};$

   (4) $\sqrt{2} \to -\sqrt{2}, \qquad \sqrt{3} \to -\sqrt{3}.$

   Since the product (composition) of any two of automorphisms (2),(3),(4) is the third, the Galois group is isomorphic to the four group (Section 1.2, Problem 6).
7. Yes, up to isomorphism. If f is the polynomial given in (3.5.11), any normal closure is a splitting field for f over F, and the result follows from (3.2.5).
8. If f is irreducible over F and has a root in $E_1 \cap E_2$, then f splits over both E_1 and E_2, hence all roots of f lie in $E_1 \cap E_2$. Thus f splits over $E_1 \cap E_2$, and the result follows.

Section 4.1

1. If $x \in R$, take $r(x+I)$ to be $rx+I$ to produce a left R-module, and $(x+I)r = xr+I$ for a right R-module. Since I is an ideal, the scalar multiplication is well-defined, and the requirements for a module can be verified using the basic properties of quotient rings.
2. If A is an algebra over F, the map $x \to x1$ of F into A is a homomorphism, and since F is a field, it is a monomorphism (see (3.1.2)). Thus A contains a copy of F. Conversely, if F is a subring of A, then A is a vector space over F, and the compatibility conditions are automatic since A is commutative.
3. Let $R = \mathbb{Z}$ and let M be the additive group of integers mod m, where m is composite, say $m = ab$ with $a, b > 1$. Take $x = a \pmod{m}$ and $r = b$.
4. Any set containing 0 is linearly dependent, so assume a/b and c/d are nonzero rationals. Since $\frac{a/b}{c/d}$ is rational, the result follows.
5. In view of Problem 4, the only hope is that a single nonzero rational number a/b spans M over $\mathbb{Z}$. But this cannot happen, since an integer multiple of a/b must be a fraction whose denominator is a divisor of b.
6. If $a \in A \subseteq C$ and $x \in B \cap C$, then $ax \in (AB) \cap C$. Conversely, let $c = ab \in (AB) \cap C$. Then $b = a^{-1}c \in C$ since $A \subseteq C$. Thus $ab \in A(B \cap C)$.

7. If $f(X) = a_0 + a_1X + \cdots + a_nX^n$ and $v \in V$, take

$$f(X)v = f(T)v = a_0Iv + a_1Tv + \cdots + a_nT^nv$$

where I is the identity transformation and T^i is the composition of T with itself i times.

Section 4.2

1. Let W be a submodule of M/N. By the correspondence theorem, $W = L/N$ for some submodule L of M with $L \geq N$. Since $L = L + N$, we have $W = (L + N)/N$.
2. No. If S is any submodule of M, then $S + N$ is a submodule of M containing N, so $S + N$ corresponds to $W = (S + N)/N$. We know that W can also be written as $(L+N)/N$ where $L \geq N$. (For example, $L = S+N$.) By the correspondence theorem, $S + N = L + N$, and there is no contradiction.
3. If $A \in M_n(R)$, then AE_{11} retains column 1 of A, with all other columns zero.
4. To identify the annihilator of E_{11}, observe that by Problem 4, $AE_{11} = 0$ iff column 1 of A is zero. For the annihilator of M, note that $E_{j1} \in M$ for every j, and AE_{j1} has column j of A as column 1, with zeros elsewhere. (See Section 2.2, Problem 4.) Thus if A annihilates everything in M, then column j of A is zero for every j, so that A is the zero matrix.
5. R/I is an R-module by Problem 1 of Section 4.1 If $r \in R$ then $r + I = r(1 + I)$, so R/I is cyclic with generator $1 + I$.
6. We must show that scalar multiplication is well-defined, that is, if $r \in I$, then $rm = 0$ for all $m \in M$. Thus I must annihilate M, in other words, $IM = 0$, where the submodule IM is the set of all finite sums $\sum r_jm_j, r_j \in R, m_j \in M$.
7. No, since $(r + I)m$ coincides with rm.

Section 4.3

1. Essentially the same proof as in (4.3.3) works. If $z_1 + \cdots + z_n = 0$, with $z_i \in M_i$, then z_n is a sum of terms from previous modules, and is therefore 0. Inductively, every z_i is 0. (In the terminology of (4.3.3), z_i is $x_i - y_i$.)
2. Only when $A = \{0\}$. If A has n elements, then by Lagrange's theorem, $nx = 0$ for every $x \in A$, so there are no linearly independent sets (except the empty set).
3. This follows because $(-s)r + rs = 0$.
4. If I is not a principal ideal, then I can never be free. For if I has a basis consisting of a single element, then I is principal, a contradiction. But by Problem 3, there cannot be a basis with more than one element. If $I = \langle a \rangle$ is principal, then I is free if and only if a is not a zero-divisor.
5. $\mathbb{Z}$, or any direct sum of copies of $\mathbb{Z}$, is a free $\mathbb{Z}$-module. The additive group of rational numbers is not a free $\mathbb{Z}$-module, by Problem 5 of Section 4.1

6. The "only if" part was done in (4.3.6), so assume that M has the given property. Construct a free module $M' = \oplus_{i \in S} R_i$ where $R_i = R$ for all i. Then the map $f\colon S \to M'$ with $f(i) = e_i$ (where e_i has 1 in its i^{th} component and zeros elsewhere) extends to a homomorphism (also called f) from M to M'. Let $g\colon M' \to M$ be the module homomorphism determined by $g(e_i) = i$. Then $g \circ f$ is the identity on S, hence on M, by the uniqueness assumption. Similarly, $f \circ g = 1$.
7. An element of M is specified by choosing a finite subset F of α, and then selecting an element $b_i \in R$ for each $i \in F$. The first choice can be made in α ways, and the second in $|R|^{|F|} = |R|$ ways. Thus $|M| = \alpha|R| = \max(\alpha, |R|)$.
8. We may take B to the set of "vectors" (e_i) with 1 in position i and zeros elsewhere. Thus there is a basis element for each copy of R, so $|B| = \alpha$.

Section 4.4

1. To prove that the condition is necessary, take the determinant of the equation $PP^{-1} = I$. Sufficiency follows from Cramer's rule.
2. A homomorphism $f\colon V \to W$ is determined by its action on elements of the form $(0, \dots, 0, x_j, 0, \dots, 0)$. Thus we must examine homomorphisms from V_j to $\oplus_{i=1}^m W_i$. Because of the direct sum, such mappings are assembled from homomorphisms from V_j to W_i, $i = 1, \dots, m$. Thus f may be identified with an $m \times n$ matrix whose ij element is a homomorphism from V_j to W_i. Formally, we have an abelian group isomorphism
$$\mathrm{Hom}_R(V, W) \cong [\mathrm{Hom}_R(V_j, W_i)].$$
3. In Problem 2, replace V and W by V^n and take all W_i and V_j to be V. This gives an abelian group isomorphism of the desired form. Now if f corresponds to $[f_{ij}]$ where $f_{ij}\colon V_j \to V_i$, and g corresponds to $[g_{ij}]$, then the composition $g \circ f$ is assembled from homomorphisms $g_{ik} \circ f_{kj}\colon V_j \to V_k \to V_i$. Thus composition of homomorphisms corresponds to multiplication of matrices, and we have a ring isomorphism.
4. In (4.4.1), take $n = m = 1$ and $M = R$.
5. Since $f(x) = f(x1) = xf(1)$, we may take $r = f(1)$.
6. This follows from Problems 3 and 4, with $V = R$.
7. If the endomorphism f is represented by the matrix A and g by B, then for any $c \in R$, we have $c(g \circ f) = (cg) \circ f = g \circ (cf)$, so $\mathrm{End}_R(M)$ is an R-algebra. Furthermore, cf is represented by cA, so the ring isomorphism is also an R-module homomorphism, hence an R-algebra isomorphism.

Section 4.5

1. Add column 2 to column 1, then add -3 times column 1 to column 2, then add -4 times row 2 to row 3. The Smith normal form is
$$S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{bmatrix}$$

2. The matrix P^{-1} is the product of the elementary column matrices in the order in which they appeared. Thus

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

$$P = \begin{bmatrix} -2 & 3 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The matrix Q is the product of the elementary row matrices in opposite order (i.e., if R_1 appears first, followed by R_2 and R_3, then $Q = R_3R_2R_1$). In this case there is only one matrix, so

$$Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{bmatrix}$$

A direct computation shows that $QAP^{-1} = S$.

3. The new basis is given by $Y = PX$, i.e., $y_1 = -2x_1 + 3x_2$, $y_2 = -x_1 + x_2$, $y_3 = x_3$. The new set of generators is given by $V = SY$, i.e., $v_1 = y_1$, $v_2 = 3y_2$, $v_3 = 6y_3$.

4. Let $d_i = a_1 \cdots a_i$. Then d_i is the gcd of the $i \times i$ minors of S, and hence of A. The a_i are recoverable from the d_i via $a_1 = d_1$ and $a_i = d_i/d_{i-1}, i > 1$. Thus the a_i are determined by the matrix A and do not depend on any particular sequence leading to a Smith normal form.

5. If A and B have the same Smith normal form S, then A and B are each equivalent to S and therefore equivalent to each other. If A and B are equivalent, then by the result stated before Problem 4, they have the same gcd of $i \times i$ minors for all i. By Problem 4, they have the same invariant factors and hence the same Smith normal form.

6. Here are the results, in sequence:

   1. The second row is now $(3\ 2\ {-13}\ 2)$
   2. The first row is $(3\ 2\ {-13}\ 2)$ and the second row is $(6\ 4\ 13\ 5)$
   3. The second row is $(0\ 0\ 39\ 1)$ and the third row is $(0\ 0\ 51\ 4)$
   4. The third row becomes $(0\ 0\ 12\ 3)$
   5. The second row is $(0\ 0\ 12\ 3)$ and the third row is $(0\ 0\ 39\ 1)$
   6. The third row is $(0\ 0\ 3\ {-8})$
   7. The second row is $(0\ 0\ 3\ {-8})$ and the third row is $(0\ 0\ 12\ 3)$
   8. The third row is $(0\ 0\ 0\ 35)$
   9. The first row is now $(3\ 2\ 2\ {-38})$
   10. The final matrix is

$$\begin{bmatrix} 3 & 2 & 2 & 32 \\ 0 & 0 & 3 & 27 \\ 0 & 0 & 0 & 35 \end{bmatrix}.$$

7. We see from the Hermite normal form that we can take $x = 0, y = 7, z = 9$, provided 0 and 35 are congruent mod m. Thus m must be 5, 7 or 35.

Section 4.6

1. $441 = 3^2 \times 7^2$, and since there are two partitions of 2, there are $2 \times 2 = 4$ mutually nonisomorphic abelian groups of order 441, with the following invariant factors:

   (1) $a_1 = 3^2 7^2$, $G \cong \mathbb{Z}_{441}$

   (2) $a_1 = 3^0 7^1$, $a_2 = 3^2 7^1$, $G \cong \mathbb{Z}_7 \oplus \mathbb{Z}_{63}$

   (3) $a_1 = 3^1 7^0$, $a_2 = 3^1 7^2$, $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{147}$

   (4) $a_1 = 3^1 7^1$, $a_2 = 3^1 7^1$, $G \cong \mathbb{Z}_{21} \oplus \mathbb{Z}_{21}$

2. $40 = 2^3 \times 5^1$, and since there are three partitions of 3 and one partition of 1, there are $3 \times 1 = 3$ mutually nonisomorphic abelian groups of order 40, with the following invariant factors:

   (1) $a_1 = 2^3 5^1$, $\quad G \cong \mathbb{Z}_{40}$

   (2) $a_1 = 2^1 5^0$, $\quad a_2 = 2^2 5^1$, $\quad G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{20}$

   (3) $a_1 = 2^1 5^0$, $\quad a_2 = 2^1 5^0$, $\quad a_3 = 2^1 5^1$, $\quad G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10}$

3. The steps in the computation of the Smith normal form are

$$\begin{bmatrix} 1 & 5 & 3 \\ 2 & -1 & 7 \\ 3 & 4 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 5 & 3 \\ 0 & -11 & 1 \\ 0 & -11 & -7 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & -11 & 1 \\ 0 & -11 & -7 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -11 \\ 0 & -7 & -11 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -11 \\ 0 & 0 & -88 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 88 \end{bmatrix}$$

   Thus $G \cong \mathbb{Z}_1 \oplus \mathbb{Z}_1 \oplus \mathbb{Z}_{88} \cong \mathbb{Z}_{88}$.

4. Cancelling a factor of 2 is not appropriate. After the relations are imposed, the group is no longer free, so that $2y = 0$ does not imply that $y = 0$. Another difficulty is that the submodule generated by $2x_1 + 2x_2 + 8x_3$ is not the same as the submodule generated by $x_1 + x_2 + 4x_3$.

5. Take $M = \oplus_{n=1}^{\infty} M_n$, where each M_n is a copy of $\mathbb{Z}$. Take $N = \mathbb{Z}$ and $P = 0$. Since the union of a countably infinite set and a finite set is still countably infinite, we have the desired result.

6. If N and P are not isomorphic, then the decompositions of N and P will involve different sequences of invariant factors. But then the same will be true for $M \oplus N$ and $M \oplus P$, so $M \oplus N$ and $M \oplus P$ cannot be isomorphic.

Section 4.7

1. If u' is another solution, then $f'u = f'u'(= vf)$, and since f' is injective, $u = u'$.

2. By commutativity, $wgfa = g'vfa$, and by exactness, $gf = 0$. Thus $vfa \in \ker g' = \operatorname{im} f'$ by exactness.
3. For commutativity, we must have $f'ua = vfa = f'a'$, so $ua = a'$. Note that a' is unique because f' is injective. Checking that u is a homomorphism is routine, e.g., if $vfa_i = f'a_i', i = 1, 2$, then $vf(a_1 + a_2) = f'(a_1' + a_2')$, so $u(a_1 + a_2) = ua_1 + ua_2$, etc.
4. $uc = ugb = g'vb$.
5. Suppose $c = gb_1 = gb_2$. Then $b_1 - b_2 \in \ker g = \operatorname{im} f$ by exactness, so $b_1 - b_2 = fa$. Then $f'wa = vfa = v(b_1 - b_2)$. By exactness, $0 = g'f'wa = g'v(b_1 - b_2)$, and the result follows.
6. Add a vertical identity map at the left side of the diagram and apply (ii) of the four lemma.
7. Add a vertical identity map at the right side of the diagram and apply (i) of the four lemma.
8. Add a vertical identity map w at the right side of the diagram and apply (ii) of the four lemma, shifting the notation $[s \to t,\ t \to u,\ u \to v,\ v \to w]$.
9. Since u and g' are surjective, v must be also, by commutativity.
10. Since f and u are injective, $f't$, hence t, must be also, by commutativity.
11. Add a vertical identity map s at the left side of the diagram, and apply (i) of the four lemma, shifting notation $[t \to s,\ u \to t,\ v \to u,\ w \to v]$.
12. If $vb = 0$, then $b = gm$, hence $0 = vgm = g'um$. Thus $um \in \ker g' = \operatorname{im} f'$, say $um = f'a'$. Since t is surjective, $a' = ta$, so $ufa = f'ta = f'a'$. Therefore um and ufa are both equal to $f'a'$. Since u is injective, $m = fa$, so $b = gm = gfa = 0$, proving that v is injective.
13. Let $a' \in A'$. Since u is surjective, $f'a' = um$, so $vgm = g'um = g'f'a' = 0$. Since v is injective, $gm = 0$, hence $m \in \ker g = \operatorname{im} f$, so $m = fa$. Thus $um = ufa = f'ta$. Therefore $f'a'$ and $f'ta$ are both equal to um. Since f' is injective, $a' = ta$, proving that t is surjective.

Section 5.1

1. The kernel of any homomorphism is a (normal) subgroup. If $g \in \ker \Phi$ then $g(xH) = xH$ for every $x \in G$, so by (1.3.1), $x^{-1}gx \in H$. Take $x = g$ to get $g \in H$.
2. By Problem 1, $\ker \Phi$ is a normal subgroup of G, necessarily proper since it is contained in H. Since G is simple, $\ker \Phi = \{1\}$, and hence Φ is injective. Since there are n left cosets of H, Φ maps into S_n.
3. If $[G : H] = n < \infty$, then by Problem 2, G can be embedded in S_n, so G is finite, a contradiction.
4. $g(xH) = xH$ iff $x^{-1}gx \in H$ iff $g \in xHx^{-1}$.
5. If $x \in G$, then $K = xKx^{-1} \subseteq xHx^{-1}$, and since x is arbitrary, $K \subseteq N$.
6. $g_1(H \cap K) = g_2(H \cap K)$ iff $g_2^{-1}g_1 \in H \cap K$ iff $g_1H = g_2H$ and $g_1K = g_2K$, proving both assertions.

7. Since $[G : H]$ and $[G : K]$ are relatively prime and divide $[G : H \cap K]$ by (1.3.5), their product divides, and hence cannot exceed, $[G : H \cap K]$.
8. By the first isomorphism theorem, G/N is isomorphic to a group of permutations of L, the set of left cosets of H. But $|L| = [G : H] = n$, so by Lagrange's theorem, $|G/N|$ divides $|S_n| = n!$.
9. Since $n > 1$, H is a proper subgroup of G, and since N is a subgroup of H, N is a proper subgroup of G as well. If $N = \{1\}$, then $|G| = [G : N]$, so by Problem 8, G divides $n!$, contradicting the hypothesis. Thus $\{1\} < N < G$, and G is not simple.

Section 5.2

1. For arbitrary σ and π, we have $\pi\sigma\pi^{-1}(\pi(i)) = \pi\sigma(i)$. In the cycle decomposition of σ, i is followed by $\sigma(i)$, and in the cycle decomposition of $\pi\sigma\pi^{-1}$, $\pi(i)$ is followed by $\pi\sigma(i)$, exactly as in the given numerical example.
2. If $g \in C_G(S)$ and $x \in S$ then $gxg^{-1} = x$, so $gSg^{-1} = S$, hence $C_G(S) \le N_G(S)$. If $g \in N_G(S)$ and $x \in S$, then $gxg^{-1} \in S$, and the action is legal. As in (5.1.3), Example 3, the kernel of the action consists of all elements of $N_G(S)$ that commute with everything in S, that is, $N_G(S) \cap C_G(S) = C_G(S)$.
3. We have $z \in G(gx)$ iff $zgx = gx$ iff $g^{-1}zgx = x$ iff $g^{-1}zg \in G(x)$ iff $z \in gG(x)g^{-1}$.
4. We have $g_1G(x) = g_2G(x)$ iff $g_2^{-1}g_1 \in G(x)$ iff $g_2^{-1}g_1x = x$ iff $g_1x = g_2x$, proving that Ψ is well-defined and injective. If the action is transitive and $y \in X$, then for some x, $y = gx = \Psi(gG(x))$ and Ψ is surjective.
5. If $g, h \in G$, then h takes gx to hgx. In the coset action, the corresponding statement is that h takes $gG(x)$ to $hgG(x)$. The formal statement is that Ψ is a"G-set isomorphism". In other words, Ψ is a bijection of the space of left cosets of $G(x)$ and X, with $\Psi(hy) = h\Psi(y)$ for all $h \in G$ and y in the coset space. Equivalently, the following diagram is commutative.

$$\begin{tikzcd}
gx \arrow[r] & hgx \\
gG(x) \arrow[u, "\Psi"] \arrow[r] & hgG(x) \arrow[u, "\Psi"']
\end{tikzcd}$$

6. The two conjugacy classes are $\{1\}$ and $G \setminus \{1\}$. Thus if $|G| = n > 1$, the orbit sizes under conjugacy on elements are 1 and $n - 1$. But each orbit size divides the order of the group, so $n - 1$ divides n. Therefore $n = k(n - 1)$, where k is a positive integer. Since $k = 1$ is not possible, we must have $k \ge 2$, so $n \ge 2(n - 1)$, so $n \le 2$.
7. If g_i is an element in the i^{th} conjugacy class, $1 \le i \le k$, then by the orbit-stabilizer theorem, the size of this class is $|G|/|C_G(g_i)|$. Since the orbits partition G, the sum of the class sizes is $|G|$, and

$$\sum_{i=1}^{k} \frac{1}{x_i} = 1$$

where $x_i = |C_G(g_i)|$. If, say, $g_1 = 1$, so that $x_1 = |G|$, the result follows from the observation that each x_i, in particular x_1, is bounded by $N(k)$.

Section 5.3

1. The group elements are I, $R = (1,2,3,4)$, $R^2 = (1,3)(2,4)$, $R^3 = (1,4,3,2)$, $F = (1)(3)(2,4)$, $RF = (1,2)(3,4)$, $R^2F = (1,3)(2)(4)$, $R^3F = (1,4)(2,3)$. Thus the number of distinct colorings is

$$\frac{1}{8}\left(n^4 + n + n^2 + n + n^3 + n^2 + n^3 + n^2\right) = \frac{1}{8}\left(n^4 + 2n^3 + 3n^2 + 2n\right).$$

2. Yes. If the vertices of the square are $1,2,3,4$ in counterclockwise order, we can identify vertex 1 with side 12, vertex 2 with side 23, vertex 3 with side 34, and vertex 4 with side 41. This gives a one-to-one correspondence between colorings in one problem and colorings in the other.
3. If the vertices of the square are $1,2,3,4$ in counterclockwise order, then $WGGW$ will mean that vertices 1 and 4 are colored white, and vertices 2 and 3 green. The equivalence classes are

$$\begin{gathered}\{WWWW\}, \{GGGG\}, \{WGGG, GWGG, GGWG, GGGW\},\\ \{GWWW, WGWW, WWGW, WWWG\},\\ \{WWGG, GWWG, GGWW, WGGW\}, \{WGWG, GWGW\}.\end{gathered}$$

4. Label $(-1,0)$ as vertex 1, $(0,0)$ as vertex 2, and $(1,0)$ as vertex 3. Then $I = (1)(2)(3)$ and $\sigma = (1,3)(2)$. Thus the number of distinct colorings is $\frac{1}{2}(n^3 + n^2)$.
5. We have free choice of color in two cycles of I and one cycle of σ. The number of distinct colorings is $\frac{1}{2}(n^2 + n)$.
6. We can generate a rotation by choosing a face of the tetrahedron to be placed on a table or other flat surface, and then choosing a rotation of 0,120 or 240 degrees. Thus there are 12 rotations, and we have enumerated all of them. By examining what each rotation does to the vertices, we can verify that all permutations are even. Since A_4 has $4!/2 = 12$ members, G must coincide with A_4, up to isomorphism.
7. The members of A_4 are $(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$, $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$, and the identity. Counting cycles of length 1, we have 11 permutations with 2 cycles and one permutation with 4 cycles. The number of distinct colorings is $\frac{1}{12}(n^4 + 11n^2)$.
8. In the above list of permutations, the first 8 have no fixed colorings. In the next 3, we can pick a cycle to be colored B, and pick a different color for the other cycle. This gives $2 \times 3 = 6$ fixed colorings. For the identity, we can pick two vertices to be colored B, and then choose a different color for each of the other two vertices. The number of fixed colorings is $\binom{4}{2}3^2 = 54$. The number of distinct colorings of the vertices is $[(6x3) + 54)]/12 = 6$.

9. As in Problem 6, a rotation can be generated by choosing a face of the cube to be placed on a table, and then choosing a rotation of 0,±90 or 180 degrees. Thus there are 24 rotations, and we have enumerated all of them. Alternatively, there is a one-to-one correspondence between rotations and permutations of the 4 diagonals of the cube. Since there are $4! = 24$ permutations of a set with 4 elements, there can be no additional rotations. The correspondence between rotations and permutations of the diagonals yields an isomorphism of G and S_4.

10. Any permutation of the faces except the identity has a cycle of length 2 or more, and each of the faces within that cycle must receive the same color, which is a contradiction. Thus $f(\pi) = 0$ for $\pi \neq I$. Now I fixes all legal colorings, and since there are 6 colors and 6 faces, the number of legal colorings is $6! = 720$. The number of distinct colorings is therefore $720/24 = 30$.

    Remark This problem can be solved directly without using the heavy machinery of this section. Without loss of generality, choose any particular color for a particular face, and move the cube so that this face is at the bottom. Choose one of the remaining 5 colors for the top face. The number of allowable colorings of the 4 remaining sides of the cube is the number of circular permutations of 4 objects, which is $3! = 6$. The number of distinct colorings is $5 \times 6 = 30$.

11. The group $G = \{1, R, R^2, \dots, R^{p-1}\}$ is cyclic of order p. Since p is prime, each R^i, $i = 1, \dots, p-1$, has order p, and therefore as a permutation of the vertices consists of a single cycle. Thus the number of distinct colorings is
$$\frac{1}{p}\left[n^p + (p-1)n\right].$$

12. Since the result of Problem 11 is an integer, $n^p + (p-1)n = n^p - n + np$ is a multiple of p, hence so is $n^p - n$. Thus for any positive integer n, $n^p \equiv n \bmod p$. It follows that if n is not a multiple of p, then $n^{p-1} \equiv 1 \bmod p$.

Section 5.4

1. Let G act on subgroups by conjugation. If P is a Sylow p-subgroup, then the stabilizer of P is $N_G(P)$ (see (5.2.2), Example 4). By (5.2.3), the index of $N_G(P)$ is n_p.

2. Since P is normal in $N_G(P)$ (see (5.2.2), Example 4), $PQ = QP \leq G$ by (1.4.3). By (5.2.4), PQ is a p-subgroup.

3. The Sylow p-subgroup P is contained in PQ, which is a p-subgroup by Problem 2. Since a Sylow p-subgroup is a p-subgroup of maximum possible size, we have $P = PQ$, and therefore $Q \subseteq P$.

4. (a) By definition of normalizer, we have $gPg^{-1} \leq gN_G(P)g^{-1} \leq gHg^{-1} = H$. Thus P and gPg^{-1} are subgroups of H, and since they are p-subgroups of maximum possible size, they are Sylow p-subgroups of H.

    (b) Since H is always a subgroup of its normalizer, let $g \in N_G(H)$. By (a), P and gPg^{-1} are conjugate in H, so for some $h \in H$ we have $gPg^{-1} = hPh^{-1}$. Thus $(h^{-1}g)P(h^{-1}g)^{-1} = P$, so $h^{-1}g \in N_G(P) \leq H$. But then $g \in H$, and the result follows.

5. By (5.2.4), $[N : P \cap N] = [PN : P] = |PN|/|P|$. Since $|P|$ is the largest possible power of p for p-subgroups of G, $[PN : P]$ and p must be relatively prime. Therefore $[N : P \cap N]$ and p are relatively prime, so $P \cap N$ is a p-subgroup of N of maximum possible size, i.e., a Sylow p-subgroup of N.
6. By the third isomorphism theorem, $[G/N : PN/N] = [G : PN] = |G|/|PN|$. Since $|G|/|P|$ and p are relatively prime and $P \leq PN$, it follows that $|G|/|PN|$ and p are relatively prime. The result follows as in Problem 5.
7. Since f is an automorphism, $f(P)$ is a subgroup of G and has the same number of elements as P, in other words, $f(P)$ is a Sylow p-subgroup. By hypothesis, $f(P) = P$.
8. By (1.3.5), $[G : N] = [G : H][H : N] = p[H : N]$, and since $[G : N]$ divides $p! = p(p-1)!$, the result follows.
9. If q is a prime factor of $[H : N]$, then by Problem 8, q is a divisor of some integer between 2 and $p-1$, in particular, $q \leq p-1$. But by Lagrange's theorem, q divides $|H|$, hence q divides $|G|$. This contradicts the fact that p is the smallest prime divisor of $|G|$. We conclude that there are no prime factors of $[H : N]$, which means that $[H : N] = 1$, Thus $H = N$, proving that H is normal in G.

Section 5.5

1. This follows from (5.5.6), part (iii), with $p = 3$ and $q = 5$.
2. Let $Z(G)a$ be a generator of $G/Z(G)$. If $g_1, g_2 \in G$, then $Z(G)g_1 = Z(G)a^i$ for some i, so $g_1a^{-i} = z_1 \in Z(G)$, and similarly $g_2a^{-j} = z_2 \in Z(G)$. Thus $g_1g_2 = a^iz_1a^jz_2 = z_1z_2a^{i+j} = z_2z_1a^{j+i} = z_2a^jz_1a^i = g_2g_1$.
3. By (5.5.3), the center $Z(G)$ is nontrivial, so has order p or p^2. In the latter case, $G = Z(G)$, so G is abelian. If $|Z(G)| = p$, then $|G/Z(G)| = p$, and $G/Z(G)$ has order p and is therefore cyclic. By Problem 2, G is abelian (and $|Z(G)|$ must be p^2, not p).
4. Each Sylow p-subgroup is of order p and therefore has $p-1$ elements of order p, with a similar statement for q and r. If we include the identity, we have $1 + n_p(p-1) + n_q(q-1) + n_r(r-1)$ distinct elements of G, and the result follows.
5. G cannot be abelian, for if so it would be cyclic of prime order. By (5.5.5), n_p, n_q and n_r are greater than 1. We know that n_p divides qr and $n_p > 1$. But n_p can't be q since $q \not\equiv 1 \bmod p$ (because $p > q$). Similarly, n_p can't be r, so $n_p = qr$. Now n_q divides pr and is greater than 1, so as above, n_q must be either p or pr (it can't be r because $q > r$, so $r \not\equiv 1 \bmod q$). Thus $n_q \geq p$. Finally, n_r divides pq and is greater than 1, so n_r is p, q, or pq. Since $p > q$, we have $n_r \geq q$.
6. Assume that G is simple. Substituting the inequalities of Problem 5 into the identity of Problem 4, we have

   $$pqr \geq 1 + qr(p-1) + p(q-1) + q(r-1).$$

   Thus

   $$0 \geq pq - p - q + 1 = (p-1)(q-1),$$

   a contradiction.

7. Since $|P| = p^r$ with $r \geq 1$ and $m > 1$, we have $1 < |P| < |G|$. Since G is simple, P is not normal in G. By (5.5.4), $n > 1$. By Problem 9 of Section 5.1, $|G|$ divides $n!$.

8. Assume G simple, and let $n = n_p$ with $p = 5$. By Sylow (2), n divides $2^4 = 16$ and $n \equiv 1 \bmod 5$. The only divisors of 16 that are congruent to 1 mod 5 are 1 and 16, and 1 is excluded by Problem 7. Thus the only possibility is $n = 16$, and by Problem 7, $2^4 5^6$ divides 16!, hence 5^6 divides 16!. But in the prime factorization of 16!, 5 appears with exponent 3 (not 6), due to the contribution of 5,10 and 15. We have reached a contradiction, so G cannot be simple.

Section 5.6

1. Apply the Jordan-Hölder theorem to the series $1 \trianglelefteq N \trianglelefteq G$.

2. $\mathbb{Z}$ has no composition series. By Section 1.1, Problem 6, each nontrivial subgroup of $\mathbb{Z}$ consists of multiples of some positive integer, so the subgroup is isomorphic to $\mathbb{Z}$ itself. Thus $\mathbb{Z}$ has no simple subgroups, so if we begin with $\{0\}$ and attempt to build a composition series, we cannot even get started.

3. We have the composition series $1 \triangleleft \mathbb{Z}_2 \triangleleft \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong Z_6$ (or $1 \triangleleft \mathbb{Z}_3 \triangleleft \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$) and $1 \triangleleft A_3 \triangleleft S_3$.

4. A_n consists of products of an even number of transpositions, and the result follows from the observation that $(a, c)(a, b) = (a, b, c)$ and $(c, d)(a, b) = (a, d, c)(a, b, c)$.

5. If $(a, b, c) \in N$ and (d, e, f) is any 3-cycle, then for some permutation π we have $\pi(a, b, c)\pi^{-1} = (d, e, f)$. Explicitly, we can take $\pi(a) = d$, $\pi(b) = e$, $\pi(c) = f$; see Section 5.2, Problem 1. We can assume without loss of generality that π is even, for if it is odd, we can replace it by $(g, h)\pi$, where g and h are not in $\{d, e, f\}$. (We use $n \geq 5$ here.) Since N is normal, $(d, e, f) \in N$.

6. If N contains $(1, 2, 3, 4)$, then it contains $(1, 2, 3)(1, 2, 3, 4)(1, 3, 2) = (1, 4, 2, 3)$, and hence contains $(1, 4, 2, 3)(1, 4, 3, 2) = (1, 2, 4)$, contradicting Problem 5. If N contains $(1, 2, 3, 4, 5)$, then it contains $(1, 2, 3)(1, 2, 3, 4, 5)(1, 3, 2) = (1, 4, 5, 2, 3)$, and so contains $(1, 4, 5, 2, 3)(1, 5, 4, 3, 2) = (1, 2, 4)$, a contradiction. The analysis for longer cycles is similar. [Actually, we should have assumed that N contains a permutation π whose disjoint cycle decomposition is $\cdots(1, 2, 3, 4)\cdots$. But multiplication by $\pi^{-1} = \cdots(1, 4, 3, 2)\cdots$ cancels the other cycles.]

7. If N contains $(1, 2, 3)(4, 5, 6)$, then it must also contain $(3, 4, 5)(1, 2, 3)(4, 5, 6)(3, 5, 4) = (1, 2, 4)(3, 6, 5)$. Thus N also contains $(1, 2, 4)(3, 6, 5)(1, 2, 3)(4, 5, 6) = (1, 4, 3, 2, 6)$, which contradicts Problem 6. If the decomposition of a permutation σ in N contains a single 3-cycle, then σ^2 *is* a 3-cycle in N, because a transposition is its own inverse. This contradicts Problem 5.

8. If, $(1, 2)(3, 4) \in N$, then $(1, 5, 2)(1, 2)(3, 4)(1, 2, 5) = (1, 5)(3, 4)$ belongs to N, and so does $(1, 5)(3, 4)(1, 2)(3, 4) = (1, 2, 5)$, contradicting Problem 5.

9. If N contains $(1, 2)(3, 4)(5, 6)(7, 8)$, then it contains

$$(2, 3)(4, 5)(1, 2)(3, 4)(5, 6)(7, 8)(2, 3)(4, 5) = (1, 3)(2, 5)(4, 6)(7, 8).$$

Therefore N contains

$$(1,3)(2,5)(4,6)(7,8)(1,2)(3,4)(5,6)(7,8) = (1,5,4)(2,3,6),$$

contradicting Problem 7.

10. We can reproduce the analysis leading to the Jordan-Hölder theorem, with appropriate notational changes. For example, we replace the "subnormal" condition $G_i \trianglelefteq G_{i+1}$ by the "normal" condition $G_i \trianglelefteq G$.
11. We say that N is a *minimal normal subgroup* of H if $\{1\} < N \trianglelefteq H$ and there is no normal subgroup of H strictly between $\{1\}$ and N. In a chief series, there can be no normal subgroup of G strictly between G_i and G_{i+1}. Equivalently, by the correspondence theorem, there is no normal subgroup of G/G_i strictly between $G_i/G_i = \{1\}$ and G_{i+1}/G_i. Thus G_{i+1}/G_i is a minimal normal subgroup of G/G_i.

Section 5.7

1. S_3 is nonabelian and solvable ($1 \triangleleft A_3 \triangleleft S_3$).
2. Let $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$ be a composition series, with all G_i/G_{i-1} cyclic of prime order (see (5.7.5)). Since $|G_i| = |G_i/G_{i-1}||G_{i-1}|$ and G_0 is finite, an induction argument shows that G is finite.
3. The factors of a composition series are simple p-groups P, which must be cyclic of prime order. For $1 \triangleleft Z(P) \trianglelefteq P$, so $Z(P) = P$ and P is abelian, hence cyclic of prime order by (5.5.1). [The trivial group is solvable with a derived series of length 0.]
4. S_3 is solvable by Problem 1, but is not nilpotent. Since S_3 is nonabelian, a central series must be of the form $1 \triangleleft H \triangleleft S_3$ with $H \subseteq Z(S_3) = 1$, a contradiction.
5. If S_n is solvable, then so is A_n by (5.7.4), and this contradicts (5.7.2).
6. By (5.5.3), P has a nontrivial center. Since $Z(P)$ is normal in P and P is simple, $Z(P) = P$ and P is abelian. By (5.5.1), P is cyclic of prime order, and since P is a p-group, the only possibility is $|P| = p$.
7. Let N be a maximal proper normal subgroup of P. (N exists because P is finite and nontrivial, and $1 \triangleleft P$.). Then the p-group P/N is simple (by the correspondence theorem). By Problem 6, $|P/N| = p$.
8. If P is a Sylow p-subgroup of G, then $|P| = p^r$ and by Problem 7, P has a subgroup Q_1 of index p, hence of order p^{r-1}. If Q_1 is nontrivial, the same argument shows that Q_1 has a subgroup Q_2 of order p^{r-2}. An induction argument completes the proof.
9. Let $G = D_6$, the group of symmetries of the equilateral triangle. Take $N = \{I, R, R^2\}$, where R is rotation by 120 degrees. Then N has index 2 in G and is therefore normal. (See Section 1.3, Problem 6, or Section 5.4, Problem 9.) Also, N has order 3 and G/N has order 2, so both N and G/N are cyclic, hence abelian. But G is not abelian, since rotations and reflections do not commute.
10. It follows from the splicing technique given in the proof of (5.7.4) that $\mathrm{dl}(G) \leq \mathrm{dl}(N) + dl(G/N)$.

Section 5.8

1. Let $H = \langle a \mid a^n \rangle$, and let C_n be a cyclic group of order n generated by a. Then $a^n = 1$ in C_n, and since $a^{n+j} = a^j$, we have $|H| \leq n = |C_n|$. The result follows as in (5.8.6).
2. The discussion in Example 4 of (2.1.3), with $i = a$ and $j = b$, shows that the quaternion group Q satisfies all the relations. Since $ab = ba^{-1}$, it follows as in (1.2.4) that every element of the given presentation H is of the form $b^r a^s, r, s \in \mathbb{Z}$. Since $b^2 = a^2$, we can restrict r to 0 or 1, and since $a^4 = 1$, we can restrict s to 0, 1, 2 or 3. Thus $|H| \leq 8$, and the result follows as in (5.8.6).
3. Take $a = (1, 2, 3)$ and $b = (1, 2)$ to show that S_3 satisfies all the relations. Since $ba = a^{-1}b$, each element of H is of the form $a^r b^s, r, s \in \mathbb{Z}$. Since $a^3 = b^2 = 1$, $|H| \leq 3 \times 2 = 6$, and the result follows as in (5.8.6).
4. No. There are many counterexamples; an easy one is $C_n = \langle a \mid a^n = 1, a^{2n} = 1 \rangle$, the cyclic group of order n.
5. $n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H = 1$.
6. Take ψ to be the inclusion map. Then $\pi\psi(h) = \pi(h) = \pi(1h) = h$. To show that π is a homomorphism, note that $n_1 h_1 n_2 h_2 = n_1(h_1 n_2 h_1^{-1}) h_1 h_2$ and $h_1 n_2 h_1^{-1} \in N$.
7. If $g \in G$ then $g = (g\pi(g)^{-1})\pi(g)$ with $\pi(g) \in H$ and $\pi(g\pi(g)^{-1}) = \pi(g)\pi(g)^{-1} = 1$, so $g\pi(g)^{-1} \in N$. [Remember that since we are taking ψ to be inclusion, π is the identity on H.] Thus $G = NH$. If $g \in N \cap H$, then $g \in \ker \pi$ and $g \in H$, so $g = \pi(g) = 1$, proving that $H \cap N = 1$.
8. If we define $\pi(n, h) = (1, h)$, $i(n, 1) = (n, 1)$, and $\psi(1, h) = (1, h)$, then the sequence of Problem 6 is exact and splits on the right.
9. We have $(n_1 h_1)(n_2 h_2) = n_1(h_1 n_2 h_1^{-1}) h_1 h_2$, so we may take $f(h)$ to be the inner automorphism of N given by conjugation by $h \in H$.
10. Consider the sequence

$$\begin{tikzcd} 1 \arrow[r] & C_3 \arrow[r, "i"] & S_3 \arrow[r, "\pi"] & C_2 \arrow[r] & 1 \end{tikzcd}$$

where C_3 consists of the identity 1 and the 3-cycles $(1, 2, 3)$ and $(1, 3, 2)$, and C_2 consists of the identity and the 2-cycle $(1, 2)$. The map i is inclusion, and π takes each 2-cycle to $(1, 2)$ and each 3-cycle to the identity. The identity map from C_2 to S_3 gives a right-splitting, but there is no left splitting. If g were a left-splitting map from S_3 to C_3, then $g(1, 2) = (1, 2, 3)$ is not possible because $g(1) = g(1, 2)g(1, 2) = (1, 2, 3)(1, 2, 3) = (1, 3, 2)$, a contradiction. Similarly, $g(1, 2) = (1, 3, 2)$ is impossible, so $g(1, 2) = 1$, so $g \circ i$ cannot be the identity. Explicitly, $g(2, 3) = g((1, 2)(1, 2, 3)) = g(1, 2, 3) = (1, 2, 3)$, and $g(1, 3) = g((1, 2)(1, 3, 2)) = g(1, 3, 2) = (1, 3, 2)$. Consequently, $g(1, 3, 2) = g((1, 3)(2, 3)) = 1$, a contradiction.

11. In the exact sequence of Problem 6, take $G = \mathbb{Z}_{p^2}$, $N = \mathbb{Z}_p$, $H = G/N \cong \mathbb{Z}_p$, i the inclusion map, and π the canonical epimorphism. If f is a right-splitting map, its image must be a subgroup with p elements (since f is injective), and there is only one such subgroup, namely $\mathbb{Z}_p$. But then $\pi \circ f = 0$, a contradiction.

12. If $g \in G$, then $gPg^{-1} \subseteq gNg^{-1} = N$, so P and gPg^{-1} are both Sylow p-subgroups of N. By Sylow (3), they are *conjugate in* N (the key point). Thus for some $n \in N$ we have $P = n(gPg^{-1})n^{-1}$. But then by definition of normalizer we have $ng \in N_G(P)$, hence $g \in NN_G(P)$.
13. The multiplication table of the group is completely determined by the relations $a^n = 1$, $b^2 = 1$, and $bab^{-1} = a^{-1}$. The relations coincide with those of D_{2n}, with $a = R$ and $b = F$.
14. The relation $a^n = 1$ disappears, and we have $\langle a, b \mid b^2 = 1, bab^{-1} = a^{-1} \rangle$.