Appendix A
The Complex Numbers

The complex numbers are an extension of the real numbers.

Definition A.1. A **complex number** is a formal expression $a + bi$, with $a, b \in \mathbb{R}$. The set of all complex numbers is denoted $\mathbb{C}$.

We define addition and multiplication on $\mathbb{C}$ via

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

and

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

for all $a, b, c, d \in \mathbb{R}$.

Example A.1. Observe that $(2+3i)+(5-9i) = 7-6i$ and $(2+3i)(5-9i) = 37-3i$.

We identify the real number a with the complex number $a+0i$. A complex number $0 + bi$, with $b \in \mathbb{R}$, is said to be **purely imaginary**. We simply write bi for such a number. In particular, note that $i^2 = -1$. Also, if $u = a + bi$, write $-u = -a - bi$.

Let us summarize a few properties concerning complex addition.

Theorem A.1. *Let $u, v, w \in \mathbb{C}$. Then*

1. $u + v \in \mathbb{C}$;
2. $u + v = v + u$;
3. $(u + v) + w = u + (v + w)$;
4. $u + 0 = u$; *and*
5. $u + (-u) = 0$.

Proof. The calculations are all straightforward. For instance, to show (2), we note that

$$(a+bi)+(c+di) = (a+c)+(b+d)i = (c+a)+(d+b)i = (c+di)+(a+bi).$$

The remaining parts are left to the reader. □

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1

Similarly, we can list some properties of complex multiplication.

Theorem A.2. *Let $u, v, w \in \mathbb{C}$. Then*

1. $uv \in \mathbb{C}$;
2. $uv = vu$;
3. $(uv)w = u(vw)$;
4. $u(v + w) = uv + uw$;
5. $1u = u$; *and*
6. *if $u \neq 0$, then there exists a $z \in \mathbb{C}$ such that $uz = 1$.*

Proof. Again, all of the calculations in (2) through (5) are straightforward. For instance, to prove (3), let $u = a + bi$, $v = c + di$ and $w = e + fi$, with $a, b, c, d, e, f \in \mathbb{R}$. Then

$$\begin{aligned}(uv)w &= ((ac - bd) + (ad + bc)i)(e + fi)\\ &= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i\\ &= (a + bi)((ce - df) + (cf + de)i)\\ &= u(vw).\end{aligned}$$

(6) If $u = a + bi$, then let $z = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$. □

(Readers who have finished Chapter 3 will realize that Theorem A.1 shows that $\mathbb{C}$ is an abelian group under addition. Those who have completed Chapter 8 will understand that the two theorems combined show that $\mathbb{C}$ is a field.)

Let us discuss a simple example of a way in which the complex numbers differ from the real numbers.

Definition A.2. If $z \in \mathbb{C}$ and n is a positive integer, then we say that z is a **primitive nth root of unity** if $z^n = 1$ but $z^m \neq 1$ for any positive integer $m < n$.

In $\mathbb{R}$, the only roots of unity are 1 and -1. But we see immediately that in $\mathbb{C}$, we have a primitive fourth root of unity, i. We can say more, however. We will need this well-known theorem due to Abraham de Moivre.

Theorem A.3 (De Moivre's Theorem). *Let $\theta \in \mathbb{R}$. Then*

$$(\cos(\theta) + \sin(\theta)i)^n = \cos(n\theta) + \sin(n\theta)i,$$

for any positive integer n.

Proof. We proceed by induction on n. If $n = 1$, there is nothing to do. Assume that the theorem holds for n. Then

$$\begin{aligned}(\cos(\theta) + \sin(\theta)i)^{n+1} &= (\cos(n\theta) + \sin(n\theta)i)(\cos(\theta) + \sin(\theta)i)\\ &= (\cos(n\theta)\cos(\theta) - \sin(n\theta)\sin(\theta))\\ &\quad + (\cos(n\theta)\sin(\theta) + \sin(n\theta)\cos(\theta))i\\ &= \cos((n + 1)\theta) + \sin((n + 1)\theta)i,\end{aligned}$$

as required. □

Corollary A.1. *Let n be a positive integer. Then* $\cos\left(\frac{2\pi}{n}\right) + \sin\left(\frac{2\pi}{n}\right) i$ *is a primitive nth root of unity in* $\mathbb{C}$.

Proof. By Theorem A.3,

$$\left(\cos\left(\frac{2\pi}{n}\right) + \sin\left(\frac{2\pi}{n}\right) i\right)^m = \cos\left(\frac{2m\pi}{n}\right) + \sin\left(\frac{2m\pi}{n}\right) i,$$

for any positive integer m. If $m = n$, then we obtain $\cos(2\pi) + \sin(2\pi)i = 1$. On the other hand, if $1 \leq m < n$, then $0 < \frac{m}{n} < 1$, and hence $\cos\left(\frac{2m\pi}{n}\right) \neq 1$. □

Example A.2. Letting $n = 3$, we obtain a primitive cube root of unity, namely, $\frac{-1}{2} + \frac{\sqrt{3}}{2} i$.

Appendix B
Matrix Algebra

Let us discuss a few definitions and basic properties of matrices. The entries in the matrices will come from rings and fields. Readers who are not yet familiar with these terms can simply assume that the entries are real numbers.

Definition B.1. Let R be a ring and m and n positive integers. Then an $m \times n$ **matrix** over R is an array of elements of R with m rows and n columns. If our matrix is A, then we write a_{ij} for the (i, j)-**entry** of A; that is,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Example B.1. If we let

$$A = \begin{pmatrix} 4 & 6 & 7 \\ 3 & 8 & 5 \end{pmatrix},$$

then A is a 2×3 matrix over $\mathbb{R}$. Furthermore, $a_{12} = 6$ and $a_{21} = 3$.

Definition B.2. Let A and B be $m \times n$ matrices over a ring R. Then their **sum** $A + B$ is the $m \times n$ matrix C such that $c_{ij} = a_{ij} + b_{ij}$ for all i and j.

Example B.2. Working with 2×2 matrices over $\mathbb{R}$, we have

$$\begin{pmatrix} 3 & 6 \\ 2 & 5 \end{pmatrix} + \begin{pmatrix} 4 & 6 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 7 & 12 \\ 3 & 7 \end{pmatrix}.$$

For any $m \times n$ matrix A, we also let $-A$ be the $m \times n$ matrix B such that $b_{ij} = -a_{ij}$ for all i and j. Furthermore, the $m \times n$ **zero matrix** has every entry 0. We denote this matrix by 0.

Let us list a few properties of matrix addition.

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1

Theorem B.1. *Let R be a ring, and m and n positive integers. If A, B and C are $m \times n$ matrices over R, then*

1. *$A + B$ is an $m \times n$ matrix over R;*
2. *$A + B = B + A$;*
3. *$(A + B) + C = A + (B + C)$;*
4. *$A + 0 = A$; and*
5. *$A + (-A) = 0$.*

Proof. The first part is contained in the definition. The other parts are all obtained by calculating the (i, j)-entry of each side. For instance, to prove (3), we note that the (i, j)-entry of $(A+B)+C$ is $(a_{ij}+b_{ij})+c_{ij}$, whereas the (i, j)-entry of $A+(B+C)$ is $a_{ij} + (b_{ij} + c_{ij})$, and these are equal. The rest of the proof is left to the reader. □

Anyone who has read Chapter 3 will note that Theorem B.1 implies that the $m \times n$ matrices over a ring form an abelian group under addition.

Definition B.3. Let A be an $m \times n$ matrix over a ring R. If $r \in R$, then the **scalar multiple** rA is the $m \times n$ matrix B such that $b_{ij} = ra_{ij}$ for all i and j.

Example B.3. Working with 3×2 matrices over $\mathbb{R}$, we have

$$5\begin{pmatrix} 1 & 3 \\ 12 & 6 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 15 \\ 60 & 30 \\ 5 & 10 \end{pmatrix}.$$

Here are a few properties of scalar multiplication.

Theorem B.2. *Let R be a ring and $m, n \in \mathbb{N}$. If A and B are $m \times n$ matrices over R and $r, s \in R$, then*

1. *rA is an $m \times n$ matrix over R;*
2. *$r(A + B) = rA + rB$;*
3. *$(r + s)A = rA + sA$; and*
4. *$r(sA) = (rs)A$.*

Proof. (1) is clear from the definition. Each of the other parts is proved by calculating the (i, j)-entry of both sides of the equation. For instance, the (i, j)-entry of $r(A+B)$ is $r(a_{ij} + b_{ij})$, whereas that of $rA + rB$ is $ra_{ij} + rb_{ij}$, but these are the same, establishing (2). The rest of the proof is left to the reader. □

If F is a field, then Theorems B.1 and B.2, when combined with the obvious fact that $1A = A$, show us that the $m \times n$ matrices over F form a vector space over F, as discussed in Chapter 12.

Matrix multiplication is a bit different.

Definition B.4. Let R be a ring, and let A be a $k \times m$ matrix over R, and B an $m \times n$ matrix over R. Then the **product** AB is the $k \times n$ matrix C such that

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{im}b_{mj},$$

for all i and j.

Example B.4. Let

$$A = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 0 & 3 \end{pmatrix} \text{ and } B = \begin{pmatrix} 3 & 4 & 1 & 5 \\ 2 & 1 & 2 & 0 \\ 1 & 2 & 6 & 1 \end{pmatrix}$$

be matrices over $\mathbb{R}$. Then

$$AB = \begin{pmatrix} 11 & 11 & 19 & 7 \\ 9 & 14 & 20 & 13 \end{pmatrix}.$$

If R is a ring with identity, then we also have the $n \times n$ **identity matrix** I_n, which is the $n \times n$ matrix A such that $a_{ii} = 1$ for all i and $a_{ij} = 0$ if $i \neq j$. For instance,

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

For any positive integer n, write $M_n(R)$ for the set of $n \times n$ matrices over a ring R.

Theorem B.3. *Let R be a ring, n a positive integer, and $A, B, C \in M_n(R)$. Then*

1. $AB \in M_n(R)$;
2. $(A + B)C = AC + BC$;
3. $A(B + C) = AB + AC$;
4. $(AB)C = A(BC)$; *and*
5. *if R is a ring with identity, then* $I_n A = AI_n = A$.

Proof. (1) follows from the definition.

(2) The (i, j)-entry of $(A + B)C$ is

$$(a_{i1} + b_{i1})c_{1j} + (a_{i2} + b_{i2})c_{2j} + \cdots + (a_{in} + b_{in})c_{nj},$$

whereas the (i, j)-entry of $AB + AC$ is

$$(a_{i1}c_{1j} + a_{i2}c_{2j} + \cdots + a_{in}c_{nj}) + (b_{i1}c_{1j} + b_{i2}c_{2j} + \cdots + b_{in}c_{nj}),$$

and these are equal.

(3) is similar to (2).

(4) Through repeated applications of (2) and (3), we can reduce (4) to the case where each of A, B and C has at most one nonzero entry. But then it is trivial.

(5) Let $D = I_n$. Then the (i, j)-entry of DA is

$$d_{i1}a_{1j} + d_{i2}a_{2j} + \cdots + d_{in}a_{nj} = a_{ij}.$$

Thus, $I_n A = A$. The proof that $AI_n = A$ is similar. □

As discussed in Chapter 8, we have now proved that if R is a ring, then so is $M_n(R)$, for any positive integer n. Furthermore, if R is a ring with identity, then so is $M_n(R)$. It is, however, worth mentioning, that $M_n(R)$ need not be commutative, even if R is. For instance, in $M_2(\mathbb{R})$,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Definition B.5. Let F be a field and n a positive integer. Then a matrix $A \in M_n(F)$ is said to be **invertible** if there exists a $B \in M_n(F)$ such that $AB = BA = I_n$. In this case, we call B the **inverse** of A and write $B = A^{-1}$.

Example B.5. In $M_2(\mathbb{R})$, the matrix

$$A = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$$

is invertible, as

$$A^{-1} = \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix}.$$

In most linear algebra courses, a couple of different methods of finding the inverse of a matrix are presented (often just in $M_n(\mathbb{R})$, but the same methods work in $M_n(F)$, for any field F). There is, however, a shortcut for determining if a matrix is invertible.

Definition B.6. Let F be a field and n a positive integer. If $A \in M_n(F)$, then the **determinant** of A, $\det(A)$, is an element of F defined recursively as follows. If $n = 1$, then $\det((a_{11})) = a_{11}$. If $n > 1$, then for any $1 \leq i, j \leq n$, let $A_{ij} \in M_{n-1}(F)$ be the matrix obtained by discarding row i and column j of A. Then

$$\det(A) = a_{11}\det(A_{11}) - a_{12}\det(A_{12}) + a_{13}\det(A_{13}) - \cdots + (-1)^{n+1}a_{1n}\det(A_{1n}).$$

Example B.6. In $M_2(F)$, we have

$$\det\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) = a_{11}a_{22} - a_{12}a_{21}.$$

Example B.7. In $M_3(\mathbb{R})$, let

$$A = \begin{pmatrix} 2 & 5 & 3 \\ 1 & 4 & 6 \\ 8 & 9 & 7 \end{pmatrix}.$$

Then

$$\begin{aligned} \det(A) &= 2\det\left(\begin{pmatrix} 4 & 6 \\ 9 & 7 \end{pmatrix}\right) - 5\det\left(\begin{pmatrix} 1 & 6 \\ 8 & 7 \end{pmatrix}\right) + 3\det\left(\begin{pmatrix} 1 & 4 \\ 8 & 9 \end{pmatrix}\right) \\ &= 2(-26) - 5(-41) + 3(-23) \\ &= 84. \end{aligned}$$

We conclude with the following result.

Theorem B.4. *Let F be a field and n a positive integer. If $A, B \in M_n(F)$, then*

1. $\det(AB) = \det(A)\det(B)$*; and*
2. *A is invertible if and only if* $\det(A) \neq 0$.

Proof. We will prove the $n = 2$ case. The general case can be found in standard introductory linear algebra textbooks.

(1) Observe that

$$AB = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Thus,

$$\det(AB) = (a_{11}b_{11} + a_{12}b_{21})(a_{21}b_{12} + a_{22}b_{22}) - (a_{11}b_{12} + a_{12}b_{22})(a_{21}b_{11} + a_{22}b_{21}).$$

On the other hand

$$\det(A)\det(B) = (a_{11}a_{22} - a_{12}a_{21})(b_{11}b_{22} - b_{12}b_{21}),$$

and these are equal.

(2) If $\det(A) \neq 0$, then let

$$B = (\det(A))^{-1} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

It is easy to verify that $AB = BA = I_2$; thus, $B = A^{-1}$. Suppose, on the other hand, that $\det(A) = 0$. If $AB = I_2$, then by (1), $\det(A)\det(B) = \det(I_2) = 1$, which is impossible. □

Solutions

Solutions to the odd-numbered problems.

Problems of Chapter 1

1.1 $S \cap T = \{3\}$, $S \cup T = \{1, 2, 3, 4\}$, $S \backslash T = \{1, 2\}$, $T \backslash S = \{4\}$ and $S \times T = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$.

1.3 Let $a \in R \cup T$. Then $a \in R$ or $a \in T$. If $a \in R$, then as $R \subseteq S$, we have $a \in S$, and hence $a \in S \cup T$. If $a \in T$, then $a \in S \cup T$.

1.5 Take $a \in R \cup (S \cap T)$. Then $a \in R$ or $a \in S \cap T$. If $a \in R$, then $a \in R \cup S$ and $a \in R \cup T$, so $a \in (R \cup S) \cap (R \cup T)$. If $a \in S \cap T$, then $a \in S$ and $a \in T$. Therefore, $a \in R \cup S$ and $a \in R \cup T$, so $a \in (R \cup S) \cap (R \cup T)$. Thus, $R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T)$. Conversely, suppose that $a \in (R \cup S) \cap (R \cup T)$. If $a \in R$, then $a \in R \cup (S \cap T)$. If $a \notin R$, then as $a \in R \cup S$, we must have $a \in S$ and, similarly, $a \in T$. Thus, $a \in S \cap T$, and hence $a \in R \cup (S \cap T)$. That is, $(R \cup S) \cap (R \cup T) \subseteq R \cup (S \cap T)$.

1.7 $(2, 3)$, $(2, 4)$, $(2, 5)$, $(3, 8)$.

1.9 Reflexive? Yes. If $a \in \mathbb{R}$, then $a - a = 0 \in \mathbb{Q}$, so $a \rho a$. Symmetric? Yes. If $a \rho b$, then $a - b \in \mathbb{Q}$, so $b - a = -(a - b) \in \mathbb{Q}$, and hence $b \rho a$. Transitive? Yes. If $a \rho b$ and $b \rho c$, then $a - b, b - c \in \mathbb{Q}$. But then $a - c = (a - b) + (b - c) \in \mathbb{Q}$, so $a \rho c$.

1.11 (1) A relation is a subset of $\{1, 2, 3\} \times \{1, 2, 3\}$. This Cartesian product has 9 elements, and therefore $2^9 = 512$ subsets. (See Exercise 1.4.)

(2) A relation ρ is symmetric provided $1 \rho 2$ if and only if $2 \rho 1$, $1 \rho 3$ if and only if $3 \rho 1$ and $2 \rho 3$ if and only if $3 \rho 2$. In short, we do not get to decide if $2 \rho 1$, $3 \rho 1$ or $3 \rho 2$, once all the other possibilities are decided. Thus, only 6 of the 9 possible pairs remain to be determined, so the total number is $2^6 = 64$.

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1

1.13 Reflexivity: As $a - a = 3 \cdot 0$, we have $a \sim a$ for all $a \in \mathbb{N}$. Symmetry: If $a \sim b$, then $a - b = 3k$, and hence $b - a = 3(-k)$; thus, $b \sim a$. Transitivity: Suppose $a \sim b$ and $b \sim c$. Then $a - b = 3k$, $b - c = 3l$, for some $k, l \in \mathbb{Z}$. Thus, $a - c = (a - b) + (b - c) = 3(k + l)$; that is, $a \sim c$. It is an equivalence relation. As for the classes, $[1] = \{1, 4, 7, \ldots\}$, $[2] = \{2, 5, 8, \ldots\}$ and $[3] = \{3, 6, 9, \ldots\}$.

1.15 Reflexivity: As $|a| = |a|$, we have $a \sim a$ for all $a \in \mathbb{Z}$. Symmetry: If $a \sim b$, then $|a| = |b|$. Therefore, $|b| = |a|$ and hence $b \sim a$. Transitivity: If $a \sim b$ and $b \sim c$ then $|a| = |b| = |c|$, and hence $a \sim c$. It is an equivalence relation. The classes are $[0] = \{0\}$, $[1] = \{1, -1\}$, $[2] = \{2, -2\}$, and so on.

1.17 Note that $\{1\}$ is a subset of $\{1, 2\}$, but $\{1, 2\}$ is not a subset of $\{1\}$. Therefore, $\sim$ is not symmetric, and hence not an equivalence relation.

1.19 Reflexivity: If $(a, b) \in \mathbb{R}^2$, then $3a-b = 3a-b$, so $(a, b) \sim (a, b)$. Symmetry: If $(a, b) \sim (c, d)$, then $3a-b = 3c-d$, so $3c-d = 3a-b$ and hence $(c, d) \sim (a, b)$. Transitivity: If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $3a - b = 3c - d = 3e - f$, and hence $(a, b) \sim (e, f)$. Also, $(a, b) \in [(4, 2)]$ if and only if $3a-b = 3\cdot 4-2 = 10$; that is, if and only if $b = 3a - 10$. Thus, $[(4, 2)] = \{(a, 3a - 10) : a \in \mathbb{R}\}$.

1.21 Let $a \sim b$ if and only if either both or neither of a and b lie in $\{1, 2, 3\}$. Reflexivity and symmetry are clear. Suppose $a \sim b$ and $b \sim c$. If $a \in \{1, 2, 3\}$, then $b \in \{1, 2, 3\}$ and hence $c \in \{1, 2, 3\}$. Similarly if $a \notin \{1, 2, 3\}$. Thus, $\sim$ is an equivalence relation. The classes are $[1] = \{1, 2, 3\}$ and $[4] = \{4, 5, 6, \ldots\}$.

1.23 If $\alpha(a) = \alpha(b)$, then $2a-1 = 2b-1$, and hence $a = b$. Thus, α is one-to-one. But there is no $a \in \{1, 2, 3, 4\}$ such that $\alpha(a) = 2$, so α is not onto.

1.25 If $\alpha(a) = \alpha(b)$, then $2^{3a-5} = 2^{3b-5}$. Taking the base 2 logarithm, we have $3a-5 = 3b-5$, and hence $a = b$. Thus, α is one-to-one. If $c \in T$, then $\alpha(((\log_2 c)+5)/3) = c$. Therefore, α is onto as well. In fact, we will use $\beta : T \to S$ given by $\beta(c) = ((\log_2 c) + 5)/3$. We have $\beta(\alpha(a)) = \beta(2^{3a-5}) = (\log_2(2^{3a-5}) + 5)/3 = a$, for all $a \in S$.

1.27 (1) and (3) are binary operations, as $ab \in \mathbb{N}$ for all $a, b \in \mathbb{N}$, and $3 \in \mathbb{N}$. But (2) is not, as $1 * 2 = -1 \notin \mathbb{N}$.

1.29 Surely β is onto. If $t \in T$, then there exists an $r \in R$ such that $(\beta\alpha)(r) = t$. But then $\beta(\alpha(r)) = t$. However, α need not be. To see this, let R and S be the set of real numbers and let T be the set of nonnegative real numbers. Let $\alpha(r) = r^2$ and $\beta(s) = s^2$. Then α is not onto, as there is no $r \in R$ such that $\alpha(r) = -1$. However, if $t \in T$, then $\beta(\alpha(\sqrt[4]{t})) = \beta(\sqrt{t}) = t$; thus, $\beta\alpha$ is onto.

1.31 (1) For each of the m elements a of S, there are n possible choices for $\alpha(a)$, so n^m.

(2) If $n < m$, the answer is 0, as the m elements of S need to map to m different places. Suppose $n \geq m$ and let $S = \{a_1, \ldots, a_m\}$. Then there are n choices for $\alpha(a_1)$, leaving $n - 1$ choices for $\alpha(a_2)$, and so on. The answer is $n(n-1)\cdots(n-m+1)$.

Problems of Chapter 2

2.1 Apply induction. When $n = 1$, both sides are 1. Assume the result for n, then prove it for $n+1$: $1+\cdots+n+(n+1) = n(n+1)/2+(n+1) = (n+1)(n+2)/2 = (n+1)((n+1)+1)/2$, as required.

2.3 (1) This is the Binomial Theorem with $a = b = 1$.
(2) This is the Binomial Theorem with $a = 1, b = -1$.

2.5 (1) By induction on n. We have nothing to prove for $n = 1$, so we begin with $n = 2$. Here, $(1+a)^2 = 1+2a+a^2 > 1+2a$, as a is positive. Assume the result for n, and prove it for $n+1$. But $(1+a)^{n+1} = (1+a)^n(1+a) > (1+na)(1+a) = 1+(n+1)a+na^2 > 1+(n+1)a$, as $a > 0$.
(2) Apply (1) with $a = (n-1)/n$, then take nth roots.

2.7 By strong induction on n. If $n = 1$ or 2, the result is obvious, so assume that $n > 2$ and the result is true for smaller n. Then $f_n = f_{n-1} + f_{n-2} \le (7/4)^{n-2} + (7/4)^{n-3} = (7/4)^{n-3}(7/4+1) < (7/4)^{n-1}$, since $11/4 < (7/4)^2$.

2.9 By strong induction on the area $a = rc$ of the bar. If the area is 1, then $r = c = 1$ and no actions are necessary. Suppose the area is $a > 1$ and the result is true for bars of smaller area. Then a break turns the bar into two bars with areas b and c, both less than a. By our inductive hypothesis, it will take $b-1$ and $c-1$ actions, respectively, to break down these two bars. We have already used 1 action, so the total is $1+(b-1)+(c-1) = (b+c)-1 = a-1$, as required. Alternative solution: We must turn 1 bar into rc bars. Each action adds one bar. So we need $rc-1$ actions.

2.11 (1) $57 = 20(2) + 17$; $20 = 17(1) + 3$; $17 = 3(5) + 2$; $3 = 2(1) + 1$; $2 = 1(2) + 0$. Thus, $(57, 20) = 1$.
(2) $117 = 51(2) + 15$; $51 = 15(3) + 6$; $15 = 6(2) + 3$; $6 = 3(2) + 0$. Thus, $(117, 51) = 3$.

2.13 Let us write $b = ac$ and $a = bd$, with $c, d \in \mathbb{Z}$. Then $a = acd$; that is, $a(1-cd) = 0$. If $a = 0$, then as $b = ac$, we have $b = 0$ as well. Otherwise, $1 - cd = 0$, so $cd = 1$. Thus, $d \in \{1, -1\}$, so $a \in \{b, -b\}$.

2.15 Let $d = (b, c)$. Then $d|c$ and $c|a$, so $d|a$. But also $d|b$. As $(a, b) = 1$, we must have $d = 1$.

2.17 If a and n are relatively prime, write $au + nv = 1$. Then $n(-v) = au - 1$. On the other hand, if $(a, n) = d > 1$ and $au - 1 = nb$, for some $b \in \mathbb{Z}$, then $1 = au - nb$. Now, $d|a$ and $d|n$, so $d|1$, which is impossible.

2.19 By strong induction on n. It is clear if $n \le 4$. So let $n > 4$ and suppose that it is true for smaller n. Then $f_n = f_{n-1} + f_{n-2} = (f_{n-2} + f_{n-3}) + f_{n-2} = 2f_{n-2} + f_{n-3} = 2(f_{n-3} + f_{n-4}) + f_{n-3} = 3f_{n-3} + 2f_{n-4}$. If $4|n$, then $4|(n-4)$, so $3|f_{n-4}$, and hence $3|f_n$. Suppose that $4 \nmid n$. Then $4 \nmid (n-4)$, so $3 \nmid f_{n-4}$. If $3|f_n$, then $3|(f_n - 3f_{n-3}) = 2f_{n-4}$. As $(3, 2) = 1$, we see that $3|f_{n-4}$, giving us a contradiction.

2.21 $3528 = 2^3 \cdot 3^2 \cdot 7^2$, $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ and $220000 = 2^5 \cdot 5^4 \cdot 11$.

2.23 Let $d = (p, n)$. As d is a positive integer and $d|p$, we can only have $d = 1$ or p. If $d = 1$, we are done. If $d = p$, then as $d|n$, we are done.

2.25 If $p_i|(p_1 \cdots p_k + 1)$, then as $p_i|p_1 \cdots p_k$, we have $p_i|(p_1 \cdots p_k + 1 - p_1 \cdots p_k) = 1$, which is impossible.

2.27 By Corollary 2.4, $p|a$. Let us say $a = pb$, with $b \in \mathbb{Z}$. Then $a^n = p^n b^n$, so $p^n|a^n$.

2.29 (1) and (2) are clearly commutative, but (3) is not, since $1 * 2 = 1$ but $2 * 1 = 2$.

2.31 (1) No. There is no $e \in \mathbb{Z}$ such that $2e + 1 = 2$.
(2) Yes, let $e = 0$. Then $a * e = a = e * a$ for all $a \in \mathbb{Z}$.

2.33 (1) 4.
(2) $(4 \cdot 5)^{25} = (-1)^{25} = -1 = 6$.

2.35 (2) We have $[a]+([b]+[c]) = [a]+[b+c] = [a+(b+c)] = [(a+b)+c] = [a+b]+[c] = ([a]+[b])+[c]$.
(4) Note that $[a] + [0] = [a + 0] = [a]$.
(5) Observe that $[a] + [-a] = [a + (-a)] = [0]$.

2.37 $2 \cdot 10 = 4 \cdot 5 = 6 \cdot 10 = 8 \cdot 15 = 12 \cdot 5 = 14 \cdot 10 = 16 \cdot 5 = 18 \cdot 10 = 0$. If $a \in \{1, 3, 7, 9, 11, 13, 17, 19\}$, there is no such b.

2.39 If $a^2 = 1$ in $\mathbb{Z}_p$, then $a^2 \equiv 1 \pmod{p}$; that is, $p|(a^2-1) = (a-1)(a+1)$. By Euclid's lemma, $p|(a-1)$ or $p|(a+1)$. That is, $a \equiv 1 \pmod{p}$ or $a \equiv -1 \equiv p-1 \pmod{p}$. If $p = 8$, then 1, 3, 5 and 7 are solutions.

2.41 Proceeding as in the proof of Theorem 2.13, we have $d_1 = 70$, $d_2 = 30$ and $d_3 = 21$. Solving $3u_1 + 70v_1 = 1$ using the Euclidean algorithm, we get $u_1 = -23$ and $v_1 = 1$. Solving $7u_2 + 30v_2 = 1$, we get $u_2 = 13$ and $v_2 = -3$. Solving $10u_3 + 21v_3 = 1$, we get $u_3 = -2$ and $v_3 = 1$. Thus, our answer is $a = 70 \cdot 1 \cdot 2 + 30(-3)(4) + 21 \cdot 1 \cdot 3 = -157$. (As our answer is only unique modulo $3 \cdot 7 \cdot 10 = 210$, we can also add 210 and get 53.)

Problems of Chapter 3

3.1 (1) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$.

(2) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$.

(3) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$.

3.3 There are n places to map 1, then $n-1$ to map 2, and so on. So there are $n!$ permutations. If we fix 2, then the other four numbers can be arranged at will, so there are $4! = 24$ possibilities.

3.5 Closure: Yes, the composition of two functions is a function. Associativity: Yes, the composition of functions is associative. Identity: Yes, we have the identity function sending each element of $\{1, 2, 3, 4, 5\}$ to itself. Inverses: No. Define $\alpha : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ via $\alpha(i) = 1$ for all i. There is no possible function $\beta : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ such that $\alpha\beta$ is the identity function.

3.7 (1)

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(2)

	(0, 0)	(1, 0)	(2, 0)	(0, 1)	(1, 1)	(2, 1)
(0, 0)	(0, 0)	(1, 0)	(2, 0)	(0, 1)	(1, 1)	(2, 1)
(1, 0)	(1, 0)	(2, 0)	(0, 0)	(1, 1)	(2, 1)	(0, 1)
(2, 0)	(2, 0)	(0, 0)	(1, 0)	(2, 1)	(0, 1)	(1, 1)
(0, 1)	(0, 1)	(1, 1)	(2, 1)	(0, 0)	(1, 0)	(2, 0)
(1, 1)	(1, 1)	(2, 1)	(0, 1)	(1, 0)	(2, 0)	(0, 0)
(2, 1)	(2, 1)	(0, 1)	(1, 1)	(2, 0)	(0, 0)	(1, 0)

3.9 Take $g_i \in G$, $h_i \in H$. Now, $(g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1)$ if and only if $(g_1g_2, h_1h_2) = (g_2g_1, h_2h_1)$; that is, if and only if $g_1g_2 = g_2g_1$ and $h_1h_2 = h_2h_1$.

3.11 (1) Division is not associative; for instance, $(1/2)/3 \neq 1/(2/3)$.
(2) There is no inverse for 2 (or anything else other than 1).

3.13 Yes. Let G be our set. If $a + bi, c + di \in G$, then $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$. Now, $(ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2) = 1 \cdot 1 = 1$, so $(a + bi)(c + di) \in G$. Complex multiplication is associative. Clearly $1 \in G$, and it will serve as the identity. If $a + bi \in G$, then $(a + bi)(a - bi) = a^2 + b^2 = 1$. Now, $a^2 + (-b)^2 = 1$, so $a - bi \in G$ and $(a + bi)^{-1} = a - bi$.

3.15 Yes. To show closure, note that $(a/p^n) + (b/p^m) = (ap^m + bp^n)/p^{m+n} \in G$. Addition of rational numbers is certainly associative, and $0 = 0/p$ is the additive identity. The additive inverse of a/p^n is $-a/p^n \in G$.

3.17 (1) $aca^{-1}b^{-1}c^{-1}$.
(2) $a^{-1}c^{-1}b^{-1}a$.

3.19

	a	b	c	d
a	d	a	b	c
b	a	b	c	d
c	b	c	d	a
d	c	d	a	b

3.21 If (1) holds, then for any $g, h \in G$, let $a = g$, $b = hg$, $c = gh$. Then $ab = ca = ghg$, so by assumption, $hg = gh$, and G is abelian. If (2) holds, then whenever $ab = ca$, we have $ab = ac$, so by cancellation, $b = c$.

3.23 (1) $|\mathbb{Z}_{12}| = 12$. Also, $|0| = 1$, $|1| = |5| = |7| = |11| = 12$, $|2| = |10| = 6$, $|3| = |9| = 4$, $|4| = |8| = 3$ and $|6| = 2$.

(2) $|\mathbb{Z}_2 \times \mathbb{Z}_4| = 8$. Also, $|(0, 0)| = 1$, $|(1, 0)| = |(1, 2)| = |(0, 2)| = 2$ and every other element has order 4.

3.25 $|a^3| = 20/(3, 20) = 20/1 = 20$, $|a^{12}| = 20/(12, 20) = 20/4 = 5$ and $|a^{15}| = 20/(15, 20) = 20/5 = 4$.

3.27 We are looking for the smallest positive integer n such that $(a, b)^n = (e, e)$; that is, such that $a^n = e$ and $b^n = e$. But $a^n = e$ if and only if $12|n$ and $b^n = e$ if and only if $18|n$. Thus, we want the smallest positive integer n divisible by both 12 and 18. The order is 36.

3.29 (1) Note that $a^n = e$ if and only if $(a^n)^{-1} = e^{-1}$; that is, if and only if $(a^{-1})^n = e$.

(2) Recall that conjugates have the same order. Also, $ab = b^{-1}(ba)b$.

3.31 First, note that $U(8)$ has exactly three elements of order 2, namely 3, 5 and 7. Suppose that a and b are distinct elements of order 2. Now, $(ab)^2 = a^2b^2 = e^2 = e$, since G is abelian. Furthermore, if $ab = e$, then $a = b^{-1} = b$, since b has order 2. But this is impossible. Thus, $|ab| = 2$. Furthermore, if $ab = a$, then $b = e$ and if $ab = b$, then $a = e$. Thus, a, b and ab are distinct elements of order 2. Let c be a fourth distinct element of order 2. By the same argument, ac has order 2. If $ac = a$, then $c = e$. If $ac = b$, then $c = a^{-1}b = ab$. If $ac = ab$, then $c = b$. None of these are true. Thus, ac is a fifth distinct element of order 2.

3.33 (1) Yes. Clearly H contains the identity matrix. If $A, B \in H$, then $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$, so $AB \in H$. Furthermore, $\det(A^{-1}) = 1/\det(A) = 1$, so $A^{-1} \in H$.

(2) No. H does not contain the identity.

(3) Yes. First, we see that $0 = 0/1 \in H$. Next, if $a/b, c/d \in H$, then $(a/b) + (c/d) = (ad + bc)/(bd) \in H$, and $-(a/b) = (-a)/b \in H$.

3.35 Let F be any flip and R any rotation. Drawing out the effects of each operation, we find that $FR = R^{-1}F$. This is RF if and only if $R = R^{-1}$. Letting $R = R_{360/n}$, we find that $R \neq R^{-1}$. Thus, no flip is central. In fact, $R = R^{-1}$ if and only if

$R = R_0$ or $R = R_{180}$. If n is odd, there is no R_{180}, so $Z(D_{2n}) = \{R_0\}$. If n is even, we see that R_{180} commutes with every flip, and surely with every rotation, so $Z(D_{2n}) = \{R_0, R_{180}\}$.

3.37 Let H and K be subgroups of G. If $a, b \in H \cap K$, then $a, b \in H$, so $ab \in H$. Similarly, $ab \in K$, and therefore $ab \in H \cap K$. By the same argument, $a^{-1} \in H$, $a^{-1} \in K$, so $a^{-1} \in H \cap K$. Finally, as H and K are subgroups, $e \in H$ and $e \in K$, so $e \in H \cap K$. The argument for an arbitrary intersection is similar.

3.39 (1) $\langle 0\rangle = \{0\}$, $\langle 1\rangle = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle = \langle 11\rangle = \langle 13\rangle = \langle 17\rangle = \langle 19\rangle = \mathbb{Z}_{20}$, $\langle 2\rangle = \langle 6\rangle = \langle 14\rangle = \langle 18\rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$, $\langle 4\rangle = \langle 8\rangle = \langle 12\rangle = \langle 16\rangle = \{0, 4, 8, 12, 16\}$, $\langle 5\rangle = \langle 15\rangle = \{0, 5, 10, 15\}$, $\langle 10\rangle = \{0, 10\}$.

(2) $\langle 1\rangle = \{1\}$, $\langle 3\rangle = \langle 11\rangle = \{1, 3, 9, 11\}$, $\langle 5\rangle = \langle 13\rangle = \{1, 5, 9, 13\}$, $\langle 7\rangle = \{1, 7\}$, $\langle 9\rangle = \{1, 9\}$, $\langle 15\rangle = \{1, 15\}$.

3.41 Label the vertices of the regular n-gon from 1 to n, counterclockwise. Then notice that a rotation leaves the vertices in counterclockwise order, whereas a flip changes them to clockwise. This makes clear what must happen in each case.

3.43 (1) We have $\langle a^1\rangle = G$, $\langle a^2\rangle = \{e, a^2, a^4, a^6, a^8, a^{10}\}$, $\langle a^3\rangle = \{e, a^3, a^6, a^9\}$, $\langle a^4\rangle = \{e, a^4, a^8\}$, $\langle a^6\rangle = \{e, a^6\}$, $\langle a^{12}\rangle = \{e\}$.

(2) As $\mathbb{Z}_{12}$ is cyclic of order 12 with generator 1, we have $\langle 1\rangle = \mathbb{Z}_{12}$, $\langle 2\rangle = \{0, 2, 4, 6, 8, 10\}$, $\langle 3\rangle = \{0, 3, 6, 9\}$, $\langle 4\rangle = \{0, 4, 8\}$, $\langle 6\rangle = \{0, 6\}$, $\langle 0\rangle = \{0\}$.

3.45 A positive integer is not relatively prime to p^n if and only if it is divisible by p. Thus, we are excluding $p, 2p, 3p, \ldots, p^n$. There are p^{n-1} such numbers.

3.47 It does follow, as $H \cap K$ is a subgroup of H, and every subgroup of a cyclic group is cyclic.

3.49 Let $G = \langle a\rangle$ be a cyclic group of order n. Now, $|a^i| = n/(n, i)$, for every integer i. In particular, each element of G has order dividing n. Now, for every k dividing n, the number of elements of order k is $\varphi(k)$. Thus, the sum of the $\varphi(k)$ is the number of elements in G, namely, n.

3.51 (1) If $a \in H \cap K$ has order n, then $\langle a\rangle$ is a subgroup of order n in both H and K. As $|H| = |K| = n$, this means that $H = K = \langle a\rangle$, which is impossible.

(2) If G has no elements of order n, we are done. Otherwise, take $a \in G$ of order n. Then $\langle a\rangle$ has $\varphi(n)$ elements of order n. If those are all of the elements in G, we are done. Otherwise, find $b \notin \langle a\rangle$ of order n. Then $\langle b\rangle$ contains $\varphi(n)$ elements of order n, and by (1), $\langle a\rangle$ and $\langle b\rangle$ have no elements of order n in common. Thus, we now have $2\varphi(n)$ elements of order n. Repeat. If the process stops, we have a multiple of $\varphi(n)$. If not, we have infinitely many.

3.53 (1) Left cosets: $0+H = \{\ldots, -4, 0, 4, 8, \ldots\}$, $1+H = \{\ldots, -3, 1, 5, 9, \ldots\}$, $2+H = \{\ldots, -2, 2, 6, 10, \ldots\}$, $3+H = \{\ldots, -1, 3, 7, 11, \ldots\}$. As G is abelian, the right cosets are the same.

(2) Left cosets: $R_0H = \{R_0, F_2\}$, $R_{90}H = \{R_{90}, F_4\}$, $R_{180}H = \{R_{180}, F_1\}$, $R_{270}H = \{R_{270}, F_3\}$. Right cosets: $HR_0 = \{R_0, F_2\}$, $HR_{90} = \{R_{90}, F_3\}$, $HR_{180} = \{R_{180}, F_1\}$, $HR_{270} = \{R_{270}, F_4\}$.

3.55 Let $G = pq$. If $H \leq G$, then $|H|$ divides $|G|$, so $|H| \in \{1, p, q, pq\}$. As H is a proper subgroup, the order is not pq. But the trivial group is cyclic, as is any group of prime order.

3.57 As $H \cap K$ is a subgroup of H and K, its order divides both 28 and 65. But $(28, 65) = 1$, so we can only have $H \cap K = \{e\}$.

3.59 By Exercise 3.30, $a_1 \cdots a_k$ has order 1 or 2. But a group of odd order has no elements of order 2.

3.61 Suppose otherwise, and let $h_1(H \cap K), \ldots, h_{n+1}(H \cap K)$ be distinct left cosets of $H \cap K$ in H. Then if $i \neq j$, we have $h_i^{-1}h_j \notin H \cap K$. Since $h_i^{-1}h_j \in H$, we have $h_i^{-1}h_j \notin K$. That is, $h_1K, \ldots, h_{n+1}K$ are distinct left cosets of K in G, contradicting the assumption that $[G : K] = n$.

Problems of Chapter 4

4.1 (1) Yes. Clearly H contains the identity matrix. If $A, B \in H$, then $\det(AB) = \det(A)\det(B) \in \mathbb{Q}$, and $\det(A^{-1}) = 1/\det(A) \in \mathbb{Q}$; thus, $AB, A^{-1} \in H$, and H is a subgroup. Also, if $C \in GL_2(\mathbb{R})$, then $\det(C^{-1}AC) = \det(C^{-1})\det(A)\det(C) = \det(A)\det(C^{-1})\det(C) = \det(AC^{-1}C) = \det(A) \in \mathbb{Q}$; thus, $C^{-1}AC \in H$, so H is normal.

(2) No, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$, which is not diagonal.

4.3 Let $N = \{e, a\}$. If $b \in G$, then $b^{-1}ab \in N$. But if $b^{-1}ab = e$, then $a = beb^{-1} = e$; impossible. Thus, $b^{-1}ab = a$, and a is central; naturally, e is always central.

4.5 Let N and K be normal subgroups of G. By Exercise 3.37, $N \cap K$ is a subgroup. Let $a \in N \cap K$ and $g \in G$. Since $a \in N$, we have $g^{-1}ag \in N$. Similarly, $g^{-1}ag \in K$, so $g^{-1}ag \in N \cap K$. The proof of the generalization is similar.

4.7 If $a \in G$, then $a^{-1}Ha$ is a subgroup of order n, so $a^{-1}Ha = H$.

4.9 If $g \in G, n \in N$, then $n^{-1}g^{-1}ng \in N$; thus, $g^{-1}ng = n(n^{-1}g^{-1}ng) \in N$.

4.11 We know that $|a|$ is divisible by 5. Also, $(aN)^5 = eN$, so $a^5 \in N$. By Lagrange's theorem, $(a^5)^{14} = e$. Thus, the order of a divides 70. So $|a| \in \{5, 10, 35, 70\}$. To see that these are all possible, let $G = \mathbb{Z}_{70}$, $N = \langle 5 \rangle$ and let a be 14, 7, 2 and 1, respectively.

4.13 For both parts, $G = D_8 \times \mathbb{Z}$ will suffice. We have $Z(G) = \langle R_{180} \rangle \times \mathbb{Z}$. As $G/Z(G)$ has order 4, it clearly satisfies (2). As for (1), it remains to show that $D_8/\langle R_{180} \rangle$ is abelian. But this can be seen by examining the group table from Exercise 4.12.

4.15 Let $|aN| = 42$. As G is finite, we know that a has finite order, and so its order is a multiple of 42, say $42n$. But then a^n has order 42. It need not hold for infinite groups. Indeed, let $G = \mathbb{Z}$, $N = \langle 42 \rangle$ and $a = 1$. We see that $|1 + N| = 42$, but every nonidentity element of G has infinite order.

4.17 By Exercise 4.16, $a^{-1}b^{-1}ab \in K$, for all $a, b \in G$. Similarly, $a^{-1}b^{-1}ab \in N$. But $K \cap N = \{e\}$, so $a^{-1}b^{-1}ab = e$, and hence $ab = ba$.

4.19 Clearly $e \in N$. If $a, b \in N$, say $a^k = b^l = e$, for some $k, l \in \mathbb{N}$, then $(ab)^{kl} = (a^k)^l(b^l)^k = e^l e^k = e$; thus, $ab \in N$. Also, $|a| = |a^{-1}|$, so $a^{-1} \in N$. Thus, N is a subgroup. As G is abelian, it is normal. Take any $c \in G$. If, for some $n \in \mathbb{N}$, we have $(cN)^n = eN$, then $c^n \in N$; that is, c^n has finite order, so $c^{nm} = e$ for some $m \in \mathbb{N}$. In other words, $c \in N$, so $cN = eN$.

4.21 (1) It is a homomorphism. Indeed, $\alpha(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b = \alpha(a) + \alpha(b)$. It is one-to-one, as if $\alpha(a) = 0$, then $\log_{10} a = 0$, so $a = 1$; that is, $\ker(\alpha) = \{1\}$. It is also onto, as if $b \in \mathbb{R}$, then $\alpha(10^b) = b$.

(2) It is not a homomorphism, as $\beta(0 + 0) = 1 \neq 2 = \beta(0) + \beta(0)$.

4.23 We have $\alpha((a, b)(c, d)) = \alpha((ac, bd)) = ac(bd)^{-1} = ab^{-1}cd^{-1}$ (since $U(16)$ is abelian), and this is $\alpha((a, b))\alpha((c, d))$. Thus, α is a homomorphism. Also, $\langle 7 \rangle = \{1, 7\}$. Now, $\alpha((a, b)) = 1$ if and only if $ab^{-1} = 1$; that is, we have the pairs $(1, 1), (3, 3), \ldots, (15, 15)$. Similarly, $\alpha((a, b)) = 7$ if and only if $a = 7b$, so we have the pairs $(7, 1), (5, 3), (3, 5), (1, 7), (15, 9), (13, 11), (11, 13), (9, 15)$.

4.25 (1) Not necessarily. For instance, H could be the trivial group.

(2) Yes. Let $h \in H$ have order n. As α is onto, say $\alpha(g) = h$. Since G is finite, $|g| < \infty$, so $|h|$ divides $|g|$. Let us say that $|g| = mn$. Then $|g^m| = n$.

4.27 Note that $gh = \alpha((g, h)) = \alpha((e, h)(g, e)) = \alpha((e, h))\alpha((g, e)) = hg$.

4.29 Let $H = G/N$. Define $\alpha : G \to H$ via $\alpha(g) = gN$. It is a homomorphism, as $\alpha(g_1g_2) = g_1g_2N = g_1Ng_2N = \alpha(g_1)\alpha(g_2)$, and $g \in \ker(\alpha)$ if and only if $gN = eN$; that is, if and only if $g \in N$.

4.31 (1) Count the elements of order 2.

(2) One is abelian and the other is not.

(3) We know that $\mathbb{Z}$ is cyclic. Suppose that $\mathbb{Z} \times \mathbb{Z} = \langle (a, b) \rangle$. Then there exists an $n \in \mathbb{Z}$ such that $(1, 0) = n(a, b)$. Since n cannot be 0, we see that $b = 0$. Similarly, $a = 0$. But this is impossible.

4.33 Define $\alpha : \mathbb{Z} \to GL_2(\mathbb{R})$ via $\alpha(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$. Note that $\alpha(a + b) = \begin{pmatrix} 1 & 0 \\ a + b & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \alpha(a)\alpha(b)$. Thus, α is a homomorphism. In particular, $\alpha(\mathbb{Z}) = G$ is a subgroup of $GL_2(\mathbb{R})$. Furthermore, if $\alpha(a)$ is the identity matrix, then $a = 0$; thus, α is one-to-one. Therefore, $\mathbb{Z}$ is isomorphic to $\alpha(\mathbb{Z}) = G$.

4.35 Define $\alpha : H \to a^{-1}Ha$ via $\alpha(h) = a^{-1}ha$. Then for any $h, k \in H$, we have $\alpha(hk) = a^{-1}hka = a^{-1}haa^{-1}ka = \alpha(h)\alpha(k)$; thus, α is a homomorphism. By definition, it is onto. Also, if $h \in \ker(\alpha)$, then $a^{-1}ha = e$; therefore, $h = aa^{-1} = e$, and α is one-to-one.

4.37 If $n > 1$ is a positive integer, then $n\mathbb{Z}$ is a proper subgroup which is infinite cyclic, and therefore isomorphic to $\mathbb{Z}$.

4.39 Define $\alpha : G \to G$ via $\alpha((a_1, a_2, \ldots)) = (0, a_1, a_2, \ldots)$. It is a homomorphism; indeed, if $a = (a_1, a_2, \ldots)$ and $b = (b_1, b_2, \ldots)$, then $\alpha(a + b) = \alpha(a) + \alpha(b) = (0, a_1 + b_1, a_2 + b_2, \ldots)$. Furthermore, it is one-to-one; if $\alpha(a) = (0, 0, \ldots)$, then clearly $a = (0, 0, \ldots)$. Thus, G is isomorphic to $\alpha(G)$, which is a proper subgroup of G.

4.41 Define $\alpha : G \to \mathbb{Z}$ via $\alpha((a, b)) = a - b$. Now, α is a homomorphism, since $\alpha((a, b) + (c, d)) = \alpha((a + c, b + d)) = (a + c) - (b + d) = (a - b) + (c - d) = \alpha((a, b)) + \alpha((c, d))$. Also, α is onto, since for any $a \in \mathbb{Z}$, $\alpha((a, 0)) = a$. Finally, the kernel is the set of all (a, b) such that $a - b = 0$; that is, $\ker(\alpha) = N$. Apply the First Isomorphism Theorem.

4.43 Define $\alpha : \mathbb{R} \to H$ via $\alpha(r) = \cos(2\pi r) + \sin(2\pi r)i$ (where we are working in radians). As $\cos^2(\theta) + \sin^2(\theta) = 1$ for any $\theta \in \mathbb{R}$, we see that $\alpha(\mathbb{R}) \subseteq H$. Furthermore, for any $a, b \in \mathbb{R}$ such that $a^2 + b^2 = 1$, we can surely find $r \in \mathbb{R}$ such that $\cos(2\pi r) = a$ and $\sin(2\pi r) = b$; thus, $\alpha(\mathbb{R}) = H$. To show that α is a homomorphism, calculate $\alpha(r + s)$ and $\alpha(r)\alpha(s)$ and use trigonometric identities. Finally, the kernel is the set of all $r \in \mathbb{R}$ such that $\cos(2\pi r) = 1$ and $\sin(2\pi s) = 0$; that is, $\ker(\alpha) = \mathbb{Z}$. Apply the First Isomorphism Theorem.

4.45 (1) If $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ commutes with $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, then $c = 0$. Similarly, $a = 0$. But matrices with $a = c = 0$ are easily seen to commute with everything in G, so those matrices form the centre.

(2) Define $\alpha : G \to \mathbb{Z} \times \mathbb{Z}$ via $\alpha\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\right) = (a, c)$. We can see that

$$\alpha\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\right) = \alpha\left(\begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}\right)$$

$$= (a + d, c + f) = \alpha\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\right) + \alpha\left(\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\right),$$

so α is a homomorphism. It is clearly onto. Furthermore, its kernel is precisely $Z(G)$, as we found in the first part. Now apply the First Isomorphism Theorem.

4.47 As $\alpha(ab) = (ab)^m = a^m b^m = \alpha(a)\alpha(b)$ (since G is abelian), we know that α is a homomorphism. If $\alpha(a) = e$, then $a^m = e$, and hence $|a|$ divides m. But by Lagrange's theorem, $|a|$ divides n as well. Since $(m, n) = 1$, we can only have $|a| = 1$. Thus, α is one-to-one. As G is finite, it must be onto as well.

4.49 Let α be an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Now, any homomorphism sends the identity to the identity. As α is one-to-one, $\alpha((1, 0)) \in \{(1, 0), (0, 1), (1, 1)\}$. Furthermore, once $\alpha((1, 0))$ is chosen, that leaves only two possibilities for $\alpha((0, 1))$. Once both of these are decided, there is only one option left for $\alpha((1, 1))$. So there are only $3 \cdot 2 = 6$ possible automorphisms. This does not mean that all of them are necessarily automorphisms, but as it happens, they are. To see this, note that every group of prime order is cyclic, and groups of order 4 are abelian. Thus, since Example 4.26 shows us that there are noncommuting automorphisms, no order less than 6 is possible. So all of the functions we have considered are actually automorphisms. Also, every group of order 6 is isomorphic to $\mathbb{Z}_6$ or D_6. As the automorphism group is nonabelian, it must be D_6.

4.51 As $\alpha(e) = e$, we see that e is in our set. If $\alpha(a) = a$ and $\alpha(b) = b$, then $\alpha(ab) = \alpha(a)\alpha(b) = ab$, so ab is in our set. Also, $\alpha(a^{-1}) = (\alpha(a))^{-1} = a^{-1}$, so a^{-1} is in our set.

4.53 As $\alpha(\langle a\rangle \times \{e\}) \subseteq \langle a\rangle \times \{e\}$, let us say that $\alpha((a, e)) = (a^i, e)$. Similarly, $\alpha((e, b)) = (e, b^j)$ and $\alpha((a, b)) = (a, b)^k$. But then $(a^i, b^j) = (a^k, b^k)$. That is, $\alpha((a, e)) = (a^k, e)$ and $\alpha((e, b)) = (e, b^k)$. Then for any $r, s \in \mathbb{Z}$, $\alpha((a^r, b^s)) = \alpha((a, e))^r \alpha((e, b))^s = (a^k, e)^r (e, b^k)^s = (a^r, b^s)^k$.

4.55 If m is an integer, then we know that $\alpha(m) = \alpha(m \cdot 1) = m \cdot \alpha(1)$. If n is a nonzero integer, then $\alpha(m) = \alpha\left(n \cdot \frac{m}{n}\right) = n\alpha\left(\frac{m}{n}\right)$. Thus, $\alpha\left(\frac{m}{n}\right) = \frac{1}{n}\alpha(m) = \frac{m}{n}\alpha(1)$.

Problems of Chapter 5

5.1 Let $H = \langle 3\rangle$ and $K = \langle 31\rangle$. We see that $|H| = 8$, $|K| = 2$. As the group is abelian, both subgroups are normal, and $H \cap K = \{1\}$. Thus $|HK| = 8 \cdot 2/1 = 16 = |U(32)|$, so $U(32) = H \times K$.

5.3 Note that $5(a, b) = (0, 0)$ if and only if $5a = 0$ and $5b = 0$. But $5a = 0$ for all a, whereas $5b = 0$ if and only if $b \in \{0, 5, 10, 15, 20\}$. Thus, $5 \cdot 5 = 25$ elements satisfy $5(a, b) = 0$. Now, these elements have order dividing 5, so we need only exclude the identity, which has order 1; thus, there are 24 elements of order 5. As $25(a, b) = (0, 0)$ for all a and b, we see that every element has order 1, 5 or 25. We have found 25 elements not having order 25, which means that $5 \cdot 25 - 25 = 100$ elements have order 25.

5.5 If $D_8 = H \times K$, then $|H||K| = 8$. As the subgroups are both proper, $|H| = 4$ and $|K| = 2$ (or vice versa). By Corollaries 4.2 and 4.3, H and K are abelian, so D_8 is abelian, giving us a contradiction.

5.7 Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $N_1 = \langle(1,0)\rangle$, $N_2 = \langle(0,1)\rangle$ and $N_3 = \langle(1,1)\rangle$. As G is abelian, normality is not an issue. We can see that $G = N_1N_2$, so surely $G = N_1N_2N_3$. Also, each $N_i \cap N_j = \{(0,0)\}$. But we cannot have $G = N_1 \times N_2 \times N_3$, since the order is wrong.

5.9 It does not follow. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $H = \mathbb{Z}_2$. Define $\alpha : G \to H$ via $\alpha((a,b)) = a+b$. We have $\alpha((a,b)+(c,d)) = a+b+c+d = \alpha((a,b))+\alpha((c,d))$, so α is a homomorphism. As $\alpha((0,0)) = 0$ and $\alpha((1,0)) = 1$, we see that α is onto. Now, $G = \langle(1,0)\rangle \times \langle(0,1)\rangle$, but $\alpha(\langle(1,0)\rangle) = \alpha(\langle(0,1)\rangle) = H$; thus, the intersection of the images is not trivial, so we do not have a direct product in H.

5.11 (1) $\mathbb{Z}_3 \times \mathbb{Z}_7$.

(2) $\mathbb{Z}_{81}$, $\mathbb{Z}_{27} \times \mathbb{Z}_3$, $\mathbb{Z}_9 \times \mathbb{Z}_9$, $\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

(3) $\mathbb{Z}_8 \times \mathbb{Z}_{25} \times \mathbb{Z}_{49}$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_{49}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_{49}$, $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{49}$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{49}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{49}$, $\mathbb{Z}_8 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \times \mathbb{Z}_7$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \times \mathbb{Z}_7$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \times \mathbb{Z}_7$, $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_7$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_7$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_7$.

5.13 As $|U(56)| = \varphi(56) = 24$, the possibilities are $\mathbb{Z}_8 \times \mathbb{Z}_3$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. But running through the elements of $U(56)$, we see that none have order larger than 6. As $\mathbb{Z}_8 \times \mathbb{Z}_3$ and $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ both have elements of order 12, it must be $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

5.15 We see that G is isomorphic to a direct product of groups of the form $\mathbb{Z}_{p^{n_i}}$, for various $n_i \in \mathbb{N}$. But if $n_i > 1$, then such a group has elements of order p^2.

5.17 Solving $5u + 7v = 1$ in $\mathbb{Z}$, one possible solution is $u = 3$, $v = -2$. Then $a = a^{5u+7v} = (a^5)^3(a^7)^{-2}$. Now $|a^{15}| = 7$ and $|a^{-14}| = |a^{21}| = 5$.

5.19 We proceed by strong induction on $|G|$. There is nothing to do if $|G| = 1$, so we start the induction with $|G| = 2$. In this case, $p = 2$ and G has an element of order 2. Let $|G| > 2$ and assume the result for groups of smaller order. If $e \neq b \in G$, then choose some prime q dividing $|b|$. Let $a = b^{|b|/q}$. Then $|a| = q$. If $q = p$, we are done. Otherwise $|G/\langle a\rangle| = |G|/q$, and this is still divisible by p. By our inductive hypothesis, $G/\langle a\rangle$ has an element $c\langle a\rangle$ of order p. Thus, $c^p \in \langle a\rangle$, so $c^{pq} = e$. Hence, $|c^q| = 1$ or p. But if $c^q = e$, then $(c\langle a\rangle)^q = e\langle a\rangle$. As $|c\langle a\rangle| = p$, this is impossible.

5.21 (1) 8, 2, 3, 3, 25, 7, 7.

(2) 2, 2, 2, 3, 9, 27.

5.23 p^3, q^2, r; p^2, p, q^2, r; p, p, p, q^2, r; p^3, q, q, r; p^2, p, q, q, r; p, p, p, q, q, r.

5.25 It is obviously the case for $n = 1$. For larger n, we claim that it is true if and only if n is a product of distinct primes. If $n = p_1 \cdots p_k$, where the p_i are all distinct, then the only possible list of elementary divisors is $p_1, \ldots, p_k$, so the groups are all isomorphic. On the other hand, if $p^2|n$ for some prime p, then we have the cyclic group of order n and $\mathbb{Z}_p \times \mathbb{Z}_{n/p}$. Since $(p, n/p) = p > 1$, we see that this group is not cyclic.

5.27 The list of elementary divisors of $G_1 \times G_2$ is obtained by combining the lists of elementary divisors of G_1 and G_2. Similarly for $G_1 \times G_3$. If these lists are the same, then deleting the elementary divisors of G_1 from each list, we see that G_2 and G_3 have the same elementary divisors, and hence are isomorphic.

5.29 We know that G is isomorphic to $\mathbb{Z}_{2^{n_1}} \times \cdots \times \mathbb{Z}_{2^{n_k}}$. If $2(a_1, \ldots, a_k) = (0, \ldots, 0)$, then $2a_i = 0$ for all i; that is, each a_i has order 1 or 2. But a cyclic group of order 2^{n_i} has only one element of order 2, so there are only two such a_i, for each i. In total, we get 2^k elements. But we must exclude the identity, so our number is $2^k - 1$.

5.31 (1) Remember that $q + \mathbb{Z} = r + \mathbb{Z}$ if and only if $q - r \in \mathbb{Z}$. This is basically the same as Example 1.19, using $\mathbb{Q}$ instead of $\mathbb{R}$.

(2) We have $b(a/b + \mathbb{Z}) = a + \mathbb{Z} = 0 + \mathbb{Z}$. Thus, $|a/b + \mathbb{Z}| \leq b$. But if $c \in \mathbb{N}$ and $c(a/b + \mathbb{Z}) = 0 + \mathbb{Z}$, then $ca/b \in \mathbb{Z}$; that is, $b|ac$. Since $(a, b) = 1$, this means that $b|c$. In particular, $c \geq b$, so the order is b.

5.33 We have $\alpha(a + b) = n(a + b) = na + nb = \alpha(a) + \alpha(b)$, so α is a homomorphism. If $a \in G$, then since G is divisible, there exists a $b \in G$ such that $nb = a$. Thus, $\alpha(b) = a$, and α is onto. But it is not necessarily an isomorphism. Let G be the Prüfer p-group and take $n = p$. Then we see that $1/p + \mathbb{Z} \in \ker(\alpha)$.

5.35 If N is a subgroup of G, take $a + N \in G/N$. Then for any $n \in \mathbb{N}$, there exists a $b \in G$ such that $nb = a$. Therefore, $n(b + N) = a + N$, and G/N is divisible. However, $\mathbb{Q}$ is divisible but $\mathbb{Z}$ is not, as there is no $b \in \mathbb{Z}$ such that $2b = 1$.

5.37 Let $G/N = \langle aN \rangle$. If $gN \in G/N$, then $gN = (aN)^k$, for some $k \in \mathbb{Z}$. That is, $g = a^k n$, for some $n \in N$. In other words, $G = \langle a \rangle N$. If $e \neq b \in \langle a \rangle \cap N$, then $b = a^l \in N$, for some $0 \neq l \in \mathbb{Z}$. If $l < 0$, then we may replace b with b^{-1}, so let $l > 0$. Then $(aN)^l = eN$, which means that aN has finite order in G/N. As $G/N = \langle aN \rangle$ and G/N is infinite cyclic, this is impossible. Therefore, $G = \langle a \rangle \times N$. It remains only to show that $\langle a \rangle$ is infinite cyclic. It is surely cyclic, and if $|a| = k$, then again, $(aN)^k = eN$ gives us a contradiction.

Problems of Chapter 6

6.1 (1) (2 4 7 6)(3 5)
(2) (1 2 5)(3 6 4)(7 8)

6.3 (1) (1 4 2)(3 6 7 5).
(2) Writing the permutation as a product of disjoint cycles, we get (1 2)(3 5 4), so the inverse is (1 2)(3 4 5).

6.5 An element of order 3 must be a product of one or more disjoint 3-cycles. Let us count the 3-cycles $(a\ b\ c)$. There are 9 choices for a, 8 for b and 7 for c. But

$(a\ b\ c) = (b\ c\ a) = (c\ a\ b)$, so we must divide by 3, giving $9 \cdot 8 \cdot 7/3 = 168$. For pairs of disjoint 3-cycles, we get $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4/(3 \cdot 3 \cdot 2) = 3360$, using the same argument and the fact that the order of the two cycles is irrelevant. Finally, to get three disjoint 3-cycles, we have $9!/(3 \cdot 3 \cdot 3 \cdot 3!) = 2240$, again noting that the three cycles can be permuted as we please. Our total is 5768.

6.7 If τ exists, then it has order k. Thus, if k is even, then τ^2 has order $k/2$, and therefore it cannot be a k-cycle. So suppose that k is odd. Let $\tau = \sigma^{(k+1)/2}$. Then $\tau^2 = \sigma^{k+1} = \sigma$, as σ has order k. Furthermore, as $2((k+1)/2) + (-1)k = 1$, we know that $((k+1)/2, k) = 1$. The preceding exercise tells us that τ is a k-cycle.

6.9 Let $|\sigma| = 105 = 3 \cdot 5 \cdot 7$. We know that $|\sigma|$ is the least common multiple of the lengths of its cycles in the disjoint cycle decomposition. The product of a 3-cycle, a 5-cycle and a 7-cycle would work, so $m = 15$ is a possibility. Can there be a smaller value? There must surely be a cycle whose length is a multiple of 7 and a divisor of 105. If it is smaller than 15, it can only be 7. Similarly for 3 and 5. Thus, $m = 15$ is the smallest possible value.

Let $|\tau| = 125$. The only way to make this happen is for the disjoint cycle decomposition for τ to include a 125-cycle. We see that $n = 125$.

6.11 (1) even
(2) odd

6.13 Without loss of generality, the possible products are $(1\ 2)(1\ 2) = (1)$, having order 1, $(1\ 2)(1\ 3) = (1\ 3\ 2)$, having order 3 and $(1\ 2)(3\ 4)$, having order 2.

6.15 It is certainly impossible if n is 2 or 3, as the groups are too small. But if $n \geq 4$, then A_n has the subgroup $\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. (It contains the identity, and closure is easily checked.) This subgroup is not cyclic. Indeed, if σ is a permutation of order 4, then its disjoint cycle decomposition is a product of one or more 4-cycles and, possibly, some 2-cycles. But a 4-cycle by itself is odd, so we need $n \geq 6$ to get something like $(1\ 2\ 3\ 4)(5\ 6) \in A_n$.

6.17 The order of an element in S_n is the least common multiple of the lengths of its disjoint cycles. If this order is odd, then these cycles all have odd length. But a cycle of odd length is even.

6.19 We see by inspection that $n = 1$ falls into the second category and $n = 2$ and 3 fall into the third category. Let $n \geq 4$. By Exercise 6.17, all elements of odd order lie in A_n. As A_n contains half the elements of S_n, we see that there are at least as many elements of even order as of odd order, and they can only be equal if every element of A_n has odd order. However, $(12)(34) \in A_n$ has order 2. So if $n \geq 4$, we are in the first category.

6.21 Such a subgroup would have index 2, and therefore be normal, by Theorem 4.1. But A_5 is simple.

6.23 It can. Note that A_6 has an isomorphic copy of A_5 as a proper subgroup. (Just use the exact same permutations as in A_5, assuming that each fixes the number 6.)

6.25 Let N be a nontrivial proper normal subgroup of A_4. By the preceding exercise, N contains no 3-cycles, so N is a subgroup of the group exhibited in Example 6.11. If it is not the same group, then it can only have order 2. But by Exercise 4.3, a normal subgroup of order 2 is central. However, the elements of order 2 in A_4 are the products of two disjoint transpositions, and these are not central. For instance, $(1\ 2)(3\ 4)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)(3\ 4)$.

6.27 In view of the preceding exercise, it suffices to show that each $(1\ i)$, $2 \leq i \leq n$, is the product of such transpositions. We proceed by induction on i, beginning with $i = 2$. There is nothing to do there, so assume the result for i and prove it for $i + 1$, when $1 < i < n$. However, $(i\ (i+1))(1\ i)(i\ (i+1)) = (1\ (i+1))$, completing the proof.

Problems of Chapter 7

7.1 Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$. Then A commutes with $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ if and only if $a = a + c$, $a + b = b + d$ and $c + d = d$; that is, if and only if $c = 0$ and $a = d$. Thus, the matrices in the centralizer have the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, where $a, b \in \mathbb{R}$ (and $a \neq 0$, so that the matrix is invertible).

7.3 We always have $C(H) \subseteq N(H)$. Let $A = \begin{pmatrix} 2 & 3 \\ 5 & 6 \end{pmatrix}$, and suppose that $B \in N(H)$. Then $B^{-1}AB \in H$, so $B^{-1}AB = A^n$, for some integer n. However, $\det(B^{-1}AB) = \det(A) = -3$, whereas $\det(A^n) = (\det(A))^n = (-3)^n$. We conclude that $n = 1$, and hence $B^{-1}AB = A$.

7.5 As always, $C(H) \subseteq N(H)$. Let $H = \{e, a\}$. If $b \in N(H)$, then $b^{-1}eb = e$ and we must have $b^{-1}ab \in H$. If $b^{-1}ab = e$, then $a = e$, which is impossible. Therefore, $b^{-1}ab = a$, and $b \in C(H)$.

7.7 Take $b \in C(a)$. As $C(a)$ is a subgroup, $b^{-1} \in C(a)$, so $b^{-1}a = ab^{-1}$. Inverting, we get $a^{-1}b = ba^{-1}$; thus, $b \in C(a^{-1})$. This means that $C(a) \subseteq C(a^{-1}) \subseteq C((a^{-1})^{-1}) = C(a)$.

7.9 (1) As H has prime order, it is abelian, so $H \leq C(H)$. In particular, $|C(H)|$ is divisible by 11 and divides 77, so it is 11 or 77. If it is 11, we must have $C(H) = H$. Otherwise, $H \leq Z(G)$. In the same way, we now have $|Z(G)| = 11$ or 77. Since G is not abelian, $Z(G) = H$. But this contradicts Corollary 4.1.

(2) Suppose otherwise. Combining (1) with Theorem 7.3, and noting that H is normal, we have G/H isomorphic to a subgroup of $\mathrm{Aut}(H)$. By Theorem 4.14, H is

isomorphic to $\mathbb{Z}_{11}$, and Theorem 4.22 tells us that $\mathrm{Aut}(H)$ is isomorphic to $U(11)$. But this is a group of order 10 and cannot have a subgroup of order 7.

7.11 $\{R_0\}, \{R_{180}\}, \{R_{90}, R_{270}\}, \{F_1, F_2\}, \{F_3, F_4\}$.

7.13 It does not follow. Let $G = S_3$, $H = \langle(1\ 3)\rangle$ and $K = \langle(1\ 3\ 2)\rangle$. Now consider the subgroups $\langle(1\ 2)\rangle$ and $\langle(2\ 3)\rangle$. As $(1\ 3)^{-1}(1\ 2)(1\ 3) = (2\ 3) = (1\ 3\ 2)^{-1}(1\ 2)(1\ 3\ 2)$, it follows immediately that these subgroups are both H- and K-conjugate. However, $H \cap K = \{(1)\}$, so they are not $(H \cap K)$-conjugate.

7.15 If each $[G : C(a)]$ in the class equation is divisible by p^2, then since $|G|$ is also divisible by p^2, we must have p^2 dividing the order of $|Z(G)|$, which is not the case. Thus, since each $[G : C(a)]$ divides p^n, one of them must be p. It follows that $|C(a)| = p^{n-1}$.

7.17 (1) No. Groups of order 25 are abelian, so all conjugacy classes would have just one element.

(2) Yes, S_3.

(3) No, the identity is always in a conjugacy class by itself.

7.19 Suppose that $b^{-1}ab = a^{-1}$. Then $b^{-2}ab^2 = b^{-1}a^{-1}b = (b^{-1}ab)^{-1} = a$. That is, $b^2 \in C(a)$. If G has odd order, so does b. Thus, write $|b| = 2m - 1$, for some $m \in \mathbb{N}$. Then $(b^2)^m = b$, so $b \in C(a)$. But then $b^{-1}ab = a$, so $a = a^{-1}$. That is, $a^2 = e$. As a has odd order, $a = e$, giving us a contradiction.

7.21 Sylow 2-subgroup: $\langle 25\rangle \times \langle 7\rangle$. Sylow 5-subgroup: $\langle(4, 0)\rangle$. Sylow 7-subgroup: $\langle(0, 2)\rangle$.

7.23 We have $|G| = 2 \cdot 3 \cdot 7^2$. The number of Sylow 7-subgroups is $1 + 7k$, for some nonnegative integer k, and divides 6. The only possible solution is $k = 0$.

7.25 Let H be a Sylow p-subgroup of G. By definition, its order is p^m, the largest power of p dividing $|G|$. Thus, $n \leq m$. By Exercise 7.16, H has a subgroup of order p^n.

7.27 By the Second Isomorphism Theorem, HN/N is isomorphic to $H/(H \cap N)$. In particular, its order divides $|H|$ and is therefore a power of p. Furthermore, $H \leq HN \leq G$, so $|G|/|HN|$ is a divisor of $|G|/|H|$. In particular, $|G|/|HN|$ is relatively prime to p. However, $[G/N : HN/N] = (|G|/|N|)/(|HN|/|N|) = |G|/|HN|$. Thus, HN/N is indeed a Sylow p-subgroup of G/N.

7.29 The number of Sylow 7-subgroups is $1 + 7k$ and divides 12. Thus, it is 1, and the Sylow 7-subgroup is normal.

7.31 The number of Sylow 17-subgroups is $1 + 17k$ and divides 256, so it is 1 or 256. If it is 1, the 17-Sylow subgroup is normal. If it is 256, then we note that each Sylow 17-subgroup is cyclic and has 16 elements of order 17. Distinct groups of prime order intersect trivially, so we have $16 \cdot 256 = 4096$ elements of order 17. This leaves only 256 other elements. But this is the size of a Sylow 2-subgroup, so there can be only one, and it is normal.

7.33 The number of Sylow p-subgroups is $1 + kp$ and divides q. If it is not 1, it is q, so $p|(q-1)$, giving us a contradiction. Thus, the Sylow p-subgroup is normal. Similarly, the number of Sylow q-subgroups is $1 + lq$ and divides p^2. Thus, it is 1, p or p^2. Suppose it is not 1. If it is p, then $q|(p-1)$, and since $(p-1)|(p^2-1)$, we have a contradiction. If it is p^2, we again obtain a contradiction. Therefore, the Sylow q-subgroup is normal as well. Thus, G is the direct product of its Sylow subgroups. Now, groups of order a prime or the square of a prime are abelian, and we are done.

7.35 The number of Sylow 3-subgroups is $1 + 3k$ and divides 19, so it is 1 or 19. If it is 1, then there are 2 elements of order 3. If it is 19, then there are 38, since subgroups of prime order intersect trivially.

7.37 Let H be a Sylow 7-subgroup and K a Sylow 17-subgroup. The number of Sylow 7-subgroups is $1 + 7k$ and divides 85, so it is 1 or 85. If it is 1, then H is normal. By Theorem 4.5, HK is a subgroup, and its order is $7 \cdot 17/1 = 119$. So assume that there are 85 Sylow 7-subgroups. Then we have $6 \cdot 85 = 510$ elements of order 7. The number of Sylow 17-subgroups is $1 + 17l$ and divides 35, so it is 1 or 35. If it is 1, then K is normal, and as above, we are done. Otherwise, we get $16 \cdot 35 = 560$ elements of order 17. But we now have too many elements.

7.39 It is not abelian, so we can rule out the two abelian groups. It has an element of order 6, namely $(R_{120}, 1)$, so we can rule out A_4. But it has no elements of order 4, unlike the group H from Example 7.14, which has $((1\ 2), 1)$. Thus, it must be D_{12}.

7.41 It suffices to show that every cyclic subgroup is normal, for then if $K \leq Q_8$ and $a \in K$, $b \in Q_8$, we have $b^{-1}ab \in \langle a \rangle \leq K$. As 1 and -1 are central, we need not worry about them. The remaining cases just involve checking, for instance, that $j^{-1}ij = -jij = kj = -i = i^{-1} \in \langle i \rangle$.

7.43 (1) We have $\alpha_{a,b}\alpha_{c,d}(x) = \alpha_{a,b}(cx+d) = a(cx+d)+b = acx+ad+b$. Thus, $\alpha_{a,b}\alpha_{c,d} = \alpha_{ac,ad+b} \in G$, since $p \nmid a$ and $p \nmid c$ imply that $p \nmid ac$; that is, ac is not 0 in $\mathbb{Z}_p$. Thus, we have closure. Composition of functions is always associative. The identity is $\alpha_{1,0}$. To find the inverse of $\alpha_{a,b}$, note that we want $ac = 1$ and $ad + b = 0$. Now, $(a, p) = 1$, so write $au + pv = 1$, for some $u, v \in \mathbb{Z}$. Thus, $au = 1$ in $\mathbb{Z}_p$. Let $c = u$. Similarly, letting $d = -ub$, we have $ad + b = -aub + b = 0$ in $\mathbb{Z}_p$. To see that the group is not abelian, note that $\alpha_{2,0}$ and $\alpha_{1,1}$ do not commute.

(2) Let $H = \{\alpha_{a,b} \in G : a \in \{1, 2, 4\}\}$. Closure checks out as above, since products of 1, 2 and 4 remain in $\{1, 2, 4\}$ in $\mathbb{Z}_7$. Clearly $\alpha_{1,0} \in H$, so $H \leq G$. There are 3 choices for a and 7 for b, so $|H| = 21$. Also, H is not abelian for the same reason given in the first part.

7.45 The number of Sylow p-subgroups is $1 + kp$ and divides q. As $p > q$, it is 1. The number of Sylow q-subgroups is $1 + lq$ and divides p, so it is 1 or p. But if it is p, then $q|(p-1)$, which is not allowed. Therefore, both Sylow subgroups are normal, and G is the direct product of $\mathbb{Z}_p$ and $\mathbb{Z}_q$, and hence isomorphic to $\mathbb{Z}_{pq}$, as $(p, q) = 1$.

Problems of Chapter 8

8.1 The addition table is found in Table 3.1. For multiplication, the table is as follows.

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

8.3 It is easy to see that R is closed under addition and contains $\{0\}$. Thus, since it is a finite set, it is an additive subgroup of $\mathbb{Z}_{15}$, which is an abelian group. Furthermore, R is closed under multiplication in $\mathbb{Z}_{15}$, and we know that this multiplication operation is associative and satisfies the distributive laws. Therefore, R is a ring. It is certainly commutative, and we can see that 6 is the identity.

8.5 It is not a ring, as it does not satisfy the distributive laws. Let $\alpha(x) = x^2$, $\beta(x) = x$ and $\gamma(x) = 2x$. Then $(\alpha \circ (\beta + \gamma))(x) = 9x^2$, but $(\alpha \circ \beta)(x) + (\alpha \circ \gamma)(x) = 5x^2$.

8.7 It is easy to see that the sum of two matrices in R also lies in R. Also, matrix addition is commutative and associative. The zero matrix is the additive identity, and negatives of matrices in R lie in R. Thus, R is an abelian group under addition. The product of two matrices in R is easily seen to be in R. Furthermore, matrix multiplication is associative and satisfies the distributive laws. Therefore, R is a ring. It contains the identity matrix, so it is a ring with identity. However, $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ do not commute, so it is not a commutative ring.

8.9 Not necessarily. Consider the additive group $\mathbb{Z}_p$, but define a multiplication operation via $ab = 0$ for all a and b. Clearly this operation is associative and the distributive laws are satisfied. Thus, we have a ring with p elements, but there is no identity.

8.11 (1) $a^2 + ba - ab - b^2$.
(2) $a^3 - a^2b - aba - ba^2 + ab^2 + bab + b^2a - b^3$.

8.13 We have $b = b1 = bac = 1c = c$.

8.15 No, use $R = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

8.17 Note that $(a+bi)-(c+di) = (a-c)+(b-d)i \in R$ and $(a+bi)(c+di) = (ac-bd)+(ad+bc)i \in R$, for all $a, b, c, d \in \mathbb{Z}$. Also, $0 \in R$. Thus, R is a subring. In addition, R is a unital subring, as it contains $1 + 0i$, the identity of $\mathbb{C}$.

8.19 Certainly R contains the zero matrix. If $a, b \in \mathbb{R}$, then $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a-b \end{pmatrix} \in R$, and $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & ab \end{pmatrix} \in R$. Thus, R is a subring. It is a ring with identity, as $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ serves as the identity. But the identity of $M_2(\mathbb{R})$ is not there, so it is not a unital subring.

8.21 We have $(0, 0) \in T$. If $r_1, r_2 \in R$, then $(r_1, 0) - (r_2, 0) = (r_1 - r_2, 0) \in T$ and $(r_1, 0)(r_2, 0) = (r_1 r_2, 0) \in T$.

8.23 We have $0 = 0a \in S$. If $r_1, r_2 \in R$, then $r_1 a - r_2 a = (r_1 - r_2)a \in S$ and $(r_1 a)(r_2 a) = (r_1 a r_2)a \in S$.

8.25 Not necessarily. Let $R = \mathbb{Q}$, $S = \mathbb{Z}$ and $a = 2$. Then $1/2 \in T$, but $(1/2)^2 \notin T$.

8.27 We have $1 \in R$. If $a + bi, c + di \in R$, then $(a + bi) - (c + di) = (a - c) + (b - d)i \in R$. Furthermore, $(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in R$. If $c + di \neq 0$, then $(c + di)(c - di) = c^2 + d^2$, which is a nonzero rational number, so the inverse of $c + di$ is $\frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i \in R$.

8.29 We have $(r, s) \in U(R \oplus S)$ if and only if there exist $r_1 \in R$, $s_1 \in S$ such that $rr_1 = r_1 r = 1$ and $ss_1 = s_1 s = 1$; that is, if and only if $r \in U(R)$ and $s \in U(S)$.

8.31 If $a^2 = a$, then $a(a - 1) = 0$, so since there are no zero divisors, $a = 0$ or 1. An integral domain must have these two elements.

8.33 By Exercise 8.20, $K \cap L$ is a subring. As $1 \in K$ and $1 \in L$, we have $1 \in K \cap L$. Also, if $0 \neq a \in K \cap L$, then $a^{-1} \in K$ and $a^{-1} \in L$, so $a^{-1} \in K \cap L$. Thus, $K \cap L$ is a subfield. The proof for an arbitrary collection of subfields is similar.

8.35 We have $(a^{10})^4 = (b^{10})^4$ and $(a^{13})^3 = (b^{13})^3$. That is, $a^{40} = b^{40}$ and $a^{39} = b^{39}$. So, $a^{39}a = b^{39}b = a^{39}b$. If $a = 0$, then since $b^{40} = 0$ and there are no zero divisors, $b = 0$. If $a \neq 0$, then cancelling a^{39}, we obtain $a = b$.

8.37 (1) 7.
(2) 0.

8.39 As 1 cannot have infinite order in a finite additive group, we know that char $R = p$, for some prime p. Thus, $pa = 0$ for all $a \in R$, so every element of R has additive order 1 or p. If $|R|$ is divisible by some prime $q \neq p$, then by Cauchy's theorem, R has an element of additive order q, which is impossible. Thus, the only prime dividing $|R|$ is p.

8.41 (1) We have $(1 + a)(1 - a + a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1}) = 1$.
(2) Let char $R = p$ and choose k such that $p^k > n$. Then $(1 + a)^{p^k} = 1 + a^{p^k}$ (using the Freshman's Dream). But $a^{p^k} = a^n a^{p^k - n} = 0$, so $(1 + a)^{p^k} = 1$.

Problems of Chapter 9

9.1 (1) $(0,0)$, $(0,1)$, $(0,2)$, $(0,3)$, $(0,4)$, $(0,5)$.
(2) $(0,0)$, $(2,0)$, $(0,3)$, $(2,3)$.

9.3 By Exercise 8.20, $I \cap J$ is a subring. Take $a \in I \cap J$ and $r \in R$. Then $a \in I$ implies $ra, ar \in I$. Similarly, $ra, ar \in J$, so $ra, ar \in I \cap J$, and $I \cap J$ is an ideal. The argument for an arbitrary collection of ideals is similar.

9.5 (1) Let $R = 2\mathbb{Z}$, $a = 2$.
(2) Let $R = M_2(\mathbb{R})$, $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Every matrix in S is of the form $\begin{pmatrix} b & 0 \\ c & 0 \end{pmatrix}$, for some $b, c \in \mathbb{R}$. Clearly $a \in S$, but multiplying on the right by $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, we get a matrix not in S, so S is not an ideal.

9.7 Let $R = \mathbb{Z}_8$, $I = (2)$ and $J = (4)$.

9.9 We know from Exercise 3.42 that G is an additive group. It is clearly abelian. It is also closed under multiplication. Furthermore, $(a_1, a_2, \ldots)((b_1, b_2, \ldots)(c_1, c_2, \ldots)) = (a_1b_1c_1, a_2b_2c_2, \ldots) = ((a_1, a_2, \ldots)(b_1, b_2, \ldots))(c_1, c_2, \ldots)$. Thus, we have associativity of multiplication. The distributive law follows similarly, and we have a ring. By Exercise 3.42, H is an additive subgroup of G, so it remains only to check absorption. If $(a_1, a_2, \ldots) \in H$, $(b_1, b_2, \ldots) \in G$, then only finitely many of the a_i are different from 0, so only finitely many of the a_ib_i are different from 0, and $(a_1b_1, a_2b_2, \ldots) \in H$. Similarly for $(b_1a_1, b_2a_2, \ldots)$.

9.11 The addition table may be found in Table 4.2 (replacing each instance of "N" with "I"). The multiplication table follows.

	$0+I$	$1+I$	$2+I$	$3+I$	$4+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$2+I$	$3+I$	$4+I$
$2+I$	$0+I$	$2+I$	$4+I$	$1+I$	$3+I$
$3+I$	$0+I$	$3+I$	$1+I$	$4+I$	$2+I$
$4+I$	$0+I$	$4+I$	$3+I$	$2+I$	$1+I$

9.13 Expanding, we obtain $8x^4+2x^3+7x^2+5x+2+I$. Now, $2(x^3+6x^2+2) \in I$, so $2x^3+I = -12x^2-4+I$. Also, $8x(x^3+6x^2+2) \in I$, so $8x^4+I = -48x^3-16x+I$. Similarly, $48x^3 + I = -288x^2 - 96 + I$. Thus, our answer is $288x^2 + 96 - 16x - 12x^2 - 4 + 7x^2 + 5x + 2 + I = 283x^2 - 11x + 94 + I$.

9.15 By the preceding exercise, $R/(I \cap J)$ is commutative if and only if $ab - ba \in I \cap J$ for all $a, b \in R$. But this happens if and only if $ab - ba \in I$ and $ab - ba \in J$ for all $a, b \in R$; that is, if and only if R/I and R/J are commutative.

9.17 The only ideals of F are $\{0\}$ and F, so 81 and 1.

9.19 If $(a+I)^n = 0+I$, then $a^n \in I$, and hence there exists an $m \in \mathbb{N}$ such that $(a^n)^m = 0$; that is, $a^{nm} = 0$, which means that $a \in I$, and hence $a+I = 0+I$.

9.21 (1) No, as $\alpha(1 \cdot 1) = 2$ but $\alpha(1)\alpha(1) = 4$.

(2) Yes. If $f(x), g(x) \in \mathbb{R}[x]$, then $\alpha(f(x)+g(x)) = f(2)+g(2) = \alpha(f(x)) + \alpha(g(x))$ and $\alpha(f(x)g(x)) = f(2)g(2) = \alpha(f(x))\alpha(g(x))$.

9.23 For any $r_1, r_2 \in R$, we have $\beta(\alpha(r_1+r_2)) = \beta(\alpha(r_1)+\alpha(r_2)) = \beta(\alpha(r_1)) + \beta(\alpha(r_2))$, and similarly for multiplication.

9.25 It is a homomorphism, as $\alpha((a,b)+(c,d)) = \alpha((a+c,b+d)) = (a+c,0) = \alpha((a,b))+\alpha((c,d))$, and similarly for multiplication. The kernel is $\{0\} \oplus \mathbb{Z}$. Furthermore, $\alpha^{-1}(2\mathbb{Z} \oplus 3\mathbb{Z}) = 2\mathbb{Z} \oplus \mathbb{Z}$.

9.27 Let $S = R/I$ and define $\alpha : R \to S$ via $\alpha(a) = a+I$. We have $\alpha(a+b) = a+b+I = (a+I)+(b+I) = \alpha(a)+\alpha(b)$, and similarly for multiplication, so α is a homomorphism. Also, $a \in \ker(\alpha)$ if and only if $a+I = 0+I$; that is, if and only if $a \in I$.

9.29 Let $\alpha : F \to K$ be a homomorphism. Now, $\ker(\alpha)$ is an ideal of F. As F is a field, this means that $\ker(\alpha) = \{0\}$ or F. In the former case, α is one-to-one, which is impossible, as K has fewer elements than F. In the latter case, $\alpha(a) = 0$ for all a, so this is the only possible homomorphism.

9.31 (1) The additive groups are not isomorphic. (See Exercise 4.31.)

(2) One has an identity, the other does not.

9.33 Let $\alpha : R \to S$ be an isomorphism. We claim that $\alpha(Z(R)) \subseteq Z(S)$. But if $a \in Z(R)$, then for any $r \in R$, we have $ar = ra$, and hence $\alpha(a)\alpha(r) = \alpha(r)\alpha(a)$. As α is onto, $\alpha(a)$ commutes with everything in S. Thus, restricting α to $Z(R)$, we have a one-to-one homomorphism into $Z(S)$. But if $b \in Z(S)$, then for any $r \in R$, we have $\alpha(r)b = b\alpha(r)$. Letting $b = \alpha(c)$, this means that $\alpha(r)\alpha(c) = \alpha(c)\alpha(r)$; that is, $\alpha(rc) = \alpha(cr)$, and since α is one-to-one, $rc = cr$. In particular, $b = \alpha(c) \in \alpha(Z(R))$. Therefore, $\alpha : Z(R) \to Z(S)$ is onto as well, and hence an isomorphism.

9.35 Let K be the field of fractions, and define $\alpha : F \to K$ via $\alpha(a) = [a,1]$ for all $a \in F$. If $a, b \in F$, then $\alpha(a+b) = [a+b,1] = [a,1]+[b,1] = \alpha(a)+\alpha(b)$ and $\alpha(ab) = [ab,1] = [a,1][b,1] = \alpha(a)\alpha(b)$; thus, α is a homomorphism. If $[a,1] = [0,1]$, then $a = 0$, so α is one-to-one. Furthermore, if $a, b \in F$, with $b \neq 0$, then $\alpha(ab^{-1}) = [ab^{-1},1] = [a,b]$; thus, α is onto.

9.37 No: $\mathbb{Z}$ and $\mathbb{Q}$ are certainly not isomorphic ($\mathbb{Q}$ is a field but $\mathbb{Z}$ is not), however, we already know that the field of fractions of $\mathbb{Z}$ is isomorphic to $\mathbb{Q}$, and by Exercise 9.35, the field of fractions of $\mathbb{Q}$ is isomorphic to $\mathbb{Q}$ as well.

9.39 (1) Note that

$$\alpha\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) = \begin{pmatrix} a+e & c+g \\ b+f & d+h \end{pmatrix} = \alpha\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) + \alpha\left(\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right).$$

Furthermore,

$$\alpha\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) = \begin{pmatrix} ae+bg & ce+dg \\ af+bh & cf+dh \end{pmatrix} = \alpha\left(\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right)\alpha\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).$$

Also, it is clear that applying α twice returns the original matrix.

(2) requires similar computations.

9.41 Define $\alpha : R \oplus S \to S$ via $\alpha((r,s)) = s$. If $r_i \in R$, $s_i \in S$, then $\alpha((r_1,s_1) + (r_2,s_2)) = \alpha((r_1+r_2, s_1+s_2)) = s_1+s_2 = \alpha((r_1,s_1)) + \alpha((r_2,s_2))$, and similarly for multiplication. Thus, α is a homomorphism. If $s \in S$, then $\alpha((0,s)) = s$, and hence α is onto. Finally, $(r,s) \in \ker(\alpha)$ if and only if $s = 0$; that is, $\ker(\alpha) = R \oplus \{0\}$. Apply the First Isomorphism Theorem.

9.43 Define $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_5$ via $\alpha(f(x)) = [f(0)]$, where the square brackets denote the congruence class in $\mathbb{Z}_5$. If $f(x), g(x) \in \mathbb{Z}[x]$, then $\alpha(f(x)+g(x)) = [f(0)+g(0)] = [f(0)] + [g(0)] = \alpha(f(x)) + \alpha(g(x))$, and similarly for multiplication. Thus, α is a homomorphism. If $[a] \in \mathbb{Z}_5$, then letting $f(x)$ be the constant polynomial a, we see that $\alpha(f(x)) = a$; thus, α is onto. Furthermore, as $f(0)$ is the constant term of $f(x)$, we see that $\ker(\alpha)$ is precisely I. Now apply the First Isomorphism Theorem.

9.45 The first part is the Third Isomorphism Theorem. To see the second part, note that $3\mathbb{Z}/12\mathbb{Z} = \{0+12\mathbb{Z}, 3+12\mathbb{Z}, 6+12\mathbb{Z}, 9+12\mathbb{Z}\}$ is a commutative ring having identity $9+12\mathbb{Z}$. Furthermore, its characteristic is 4. Thus, it has a subring isomorphic to $\mathbb{Z}_4$. As the ring only has four elements, the ring is itself isomorphic to $\mathbb{Z}_4$.

9.47 Note that $(1+i)(1-i) = 2 \in (2)$, and yet neither $1+i$ nor $1-i$ is a multiple of 2 in R. The ideal is not prime and hence, as R is a commutative ring with identity, not maximal.

9.49 Let I be a prime ideal. Then R/I is an integral domain. But a finite integral domain is a field (see Theorem 8.10), so R/I is a field, and hence I is maximal.

9.51 Let $R = 2\mathbb{Z}_4 = \{0, 2\}$ and $I = \{0\}$. Now, I is surely maximal, since if it got any larger, it would be R. But it is not prime, as $2 \notin I$, but $2 \cdot 2 = 0 \in I$.

9.53 In a field, the only element that is not a unit is 0, and $\{0\}$ is an ideal. In $\mathbb{Z}_{p^n}$, we know (see Exercise 8.30) that the units are precisely the elements a that are relatively prime to p^n. In other words, the elements that are not units are those that are divisible by p, so (p) is the ideal in question.

9.55 Use $P = R \oplus I$. As $I \neq R$, we see that $P \neq R \oplus R$. Also, if $(a,b)(c,d) \in P$, then $bd \in I$. As I is prime, either b or d is in I, and hence (a,b) or (c,d) is in P.

Problems of Chapter 10

10.1 $f(x) - g(x) = 9x^4 + 8x^3 + 4x^2 + 6x + 4$, $f(x)g(x) = 4x^7 + 7x^6 + 2x^5 + x^4 + 7x^2 + 4x + 5$.

10.3 $q(x) = 5x^2 + 6x + 3$, $r(x) = 4x^2 + 1$.

10.5 No. According to the preceding exercise, x is not a unit.

10.7 Suppose that char $R[x] = n > 0$. Then, in particular, for every constant polynomial a, we have $na = 0$. Thus, $0 < \text{char } R \leq n$. On the other hand, if char $R = m > 0$, then for any $f(x) \in R[x]$, we note that for each coefficient a_i appearing in $f(x)$, we have $ma_i = 0$; thus, $mf(x) = 0$, and $0 < \text{char } R[x] \leq m$. The only remaining case is where char R and char $R[x]$ are both 0.

10.9 Certainly $0 \in S[x]$. Take $f(x), g(x) \in S[x]$. Then all coefficients of $f(x)$ and $g(x)$ lie in S. The coefficients of $f(x) - g(x)$ are differences of elements of S, and hence lie in S, so $f(x) - g(x) \in S[x]$. Similarly, the coefficients of $f(x)g(x)$ are sums of products of elements of S and thus lie in S. Hence, $S[x]$ is a subring. Let S be an ideal. If $f(x) \in S[x]$ and $g(x) \in R[x]$, then the coefficients of $f(x)g(x)$ are sums of products, where each term in the sum is an element of S multiplied by an element of R, and therefore lies in S. Thus, $f(x)g(x) \in S[x]$. Similarly, $g(x)f(x) \in S[x]$.

10.11 As a and ab are associates, write $ab = au$, where u is a unit. If $a \neq 0$, then cancellation gives $b = u$.

10.13 Let a be a unit. Then for any $0 \neq b \in R$, we have $b = a(a^{-1}b)$. Thus, $\varepsilon(a) \leq \varepsilon(b)$, so $\varepsilon(a)$ is indeed the smallest possible value, n. Now suppose that a is not a unit. We can write $1 = aq + r$, where $q, r \in R$ and either $r = 0$ or $\varepsilon(r) < \varepsilon(a)$. In the former case, a is a unit, which is a contradiction. In the latter case, $\varepsilon(a)$ is not the smallest possible value.

10.15 We have

$$f(x) = g(x)\left(\frac{3}{2}\right) + \left(-\frac{7}{2}x^3 - \frac{13}{2}x^2 - \frac{19}{2}x + \frac{3}{2}\right)$$
$$g(x) = \left(-\frac{7}{2}x^3 - \frac{13}{2}x^2 - \frac{19}{2}x + \frac{3}{2}\right)\left(-\frac{4}{7}x - \frac{46}{49}\right) + \left(\frac{72}{49}x^2 + \frac{144}{49}x + \frac{216}{49}\right),$$

and since $\frac{72}{49}x^2 + \frac{144}{49}x + \frac{216}{49}$ divides $-\frac{7}{2}x^3 - \frac{13}{2}x^2 - \frac{19}{2}x + \frac{3}{2}$, the former is a gcd. We must make it monic, so multiplying by $49/72$, we get $(f(x), g(x)) = x^2 + 2x + 3$.

10.17 Beginning with the second of the two equations in the solution to Exercise 10.15, we see that

$$\begin{aligned}(f(x), g(x)) &= \frac{49}{72}\left(g(x) - \left(-\frac{7}{2}x^3 - \frac{13}{2}x^2 - \frac{19}{2}x + \frac{3}{2}\right)\left(-\frac{4}{7}x - \frac{46}{49}\right)\right) \\ &= \frac{49}{72}\left(g(x) - \left(f(x) - g(x)\left(\frac{3}{2}\right)\right)\left(-\frac{4}{7}x - \frac{46}{49}\right)\right) \\ &= f(x)\left(\frac{7}{18}x + \frac{23}{36}\right) + g(x)\left(-\frac{7}{12}x - \frac{5}{18}\right).\end{aligned}$$

10.19 We must apply the Euclidean algorithm. Let us use the notation established in Example 10.8, taking $u = 5 + 7i$ and $v = 1 + 3i$. Now, $(1 + 3i)(1 - 3i) = 10$, so $uv^{-1} = (5 + 7i)(1 - 3i)/10 = 2.6 - 0.8i$. Thus, we have $m = 3$ and $n = -1$, so $q = 3 - i$ and $r = (5 + 7i) - (1 + 3i)(3 - i) = -1 - i$. That is,

$$5 + 7i = (1 + 3i)(3 - i) + (-1 - i).$$

For the next step, we let $u = 1 + 3i$ and $v = -1 - i$. But $(-1 - i)(-1 + i) = 2$, so $uv^{-1} = (1 + 3i)(-1 + i)/2 = -2 - i$. Therefore,

$$1 + 3i = (-1 - i)(-2 - i) + 0.$$

Thus, $-1 - i$ is a gcd of $5 + 7i$ and $1 + 3i$.

10.21 Using the notation as in Example 10.15, we note that $N(1 + 2\sqrt{5}i) = 21$. If $1 + 2\sqrt{5}i = uv$, then $N(u)N(v) = 21$, and assuming without loss of generality that $N(u) \leq N(v)$, we have $N(u) = 1$ or 3. As in Example 10.15, $N(u) = 3$ is impossible and $N(u) = 1$ means $u \in \{1, -1\}$. In particular, u is a unit and $1 + 2\sqrt{5}i$ is irreducible. However, $(1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i) = 21 = 3 \cdot 7$. Thus, $(1 + 2\sqrt{5}i)|21$. But as $N(3) = 9$ and $N(7) = 49$, we cannot possibly have $1 + 2\sqrt{5}i$ dividing 3 or 7. Thus, $1 + 2\sqrt{5}i$ is not prime.

10.23 Combine the preceding two exercises with Theorem 10.11.

10.25 Not necessarily. We know that $\mathbb{Z}$ is a Euclidean domain, but $\mathbb{Z}[x]$ is not a PID, hence not a Euclidean domain.

10.27 This is essentially the same as Exercise 2.24.

10.29 Suppose not, and let $0 \neq a \in R$ be a nonunit. Let $I_n = (a^n)$. As $a^n | a^{n+1}$, we see that $I_{n+1} \subseteq I_n$. Suppose that $I_n = I_{n+1}$. Then $a^n \in (a^{n+1})$; that is, $a^n = a^{n+1}b$, for some $b \in R$. Cancelling a^n, we get $1 = ab$. Thus, a is a unit, giving us a contradiction.

10.31 Using the notation in Example 10.8, we have $\varepsilon(1 + i) = 2$. As we noted in that example, if u and v are in our ring, and $uv = 1 + i$, then $\varepsilon(u)\varepsilon(v) = 2$. But $\varepsilon(u)$ and $\varepsilon(v)$ are nonnegative integers, so without loss of generality, $\varepsilon(u) = 1$. This means $u \in \{\pm 1, \pm i\}$, and so u is a unit. Thus, $1 + i$ is irreducible. However, we know that R is a Euclidean domain, and hence a PID, so every irreducible is prime, by Theorem 10.11.

10.33 Not necessarily. We know that $\mathbb{Q}[x]$ is a UFD, and yet its subring R discussed in Example 10.18 is not.

10.35 Let $a = 2$, $b = 5$, $c = 2 + \sqrt{6}i$ and $d = 2 - \sqrt{6}i$. Clearly $ab = cd = 10$. Defining a norm as in Example 10.15 via $N(m + n\sqrt{6}i) = m^2 + 6n^2$, we see from the same calculation that $N(uv) = N(u)N(v)$ for all $u, v \in R$. Suppose that $uv = 2$. Then $N(u)N(v) = 4$, so either $N(u) = N(v) = 2$ (which is impossible) or $N(u) = 1$ and $N(u) = 4$ (or vice versa). But this means u is 1 or -1. In particular, u is a unit, so 2 is irreducible. Similar calculations show that b, c and d are irreducible. It is immediate that neither a nor b divides c or d. That R is not a UFD follows from the definition.

10.37 Let p be an irreducible of R. Then p is a nonzero nonunit. Suppose that $p|ab$, for some $a, b \in R$. If a is a unit, then b and ab are associates, so $p|b$. If $a = 0$, then $p|a$. Similarly if b is zero or a unit. So let a and b be nonzero nonunits. We may write $a = p_1 \cdots p_k$ and $b = q_1 \cdots q_l$, where the p_i and q_j are irreducible. By the preceding exercise, p divides some p_i or some q_j. Without loss of generality, say $p|q_1$. Since $q_1|b$, we have $p|b$.

Problems of Chapter 11

11.1 (1) As 5 is a root and the degree is greater than 1, no.

(2) Trying each possible root in $\mathbb{Z}_7$, we see that this polynomial has no root there. Thus, since the degree is 3, it is irreducible.

(3) No, since it factors as $(x^2 + 4)(x^2 + 4)$.

11.3 The possibilities are $x^3 + ax^2 + bx + c$, where $a, b, c \in \{0, 1\}$. If $c = 0$, then 0 is a root, so $c = 1$. Also, 1 is a root of $x^3 + 1$ and $x^3 + x^2 + x + 1$, so we can rule them out. The remaining polynomials are $x^3 + x^2 + 1$ and $x^3 + x + 1$. Both have degree 3, and neither has a root, so they are irreducible.

11.5 Let $h(x) = f(x) - g(x)$. If $f(x) \neq g(x)$, then $h(x)$ is not the zero polynomial. Say $\deg(h(x)) = n$. Then $h(x)$ can have at most n roots, but $h(a) = f(a) - g(a) = 0$ for all $a \in F$, giving us a contradiction.

11.7 No, take $a, b \in R$ such that $ab \neq ba$. Let $r = a$, $f(x) = x$ and $g(x) = b$. Then $\alpha(f(x)g(x)) = \alpha(bx) = ba$, whereas $\alpha(f(x))\alpha(g(x)) = ab$.

11.9 As $\deg(x^2 + 1) = 2$, the polynomial is reducible if and only if it has a root $m \in \{0, 1, \ldots, p - 1\}$. Factoring out $x - m$, we can only be left with $x - n$, for some $n \in \{0, 1, \ldots, p - 1\}$. Thus, $x^2 + 1 = x^2 - (m + n)x + mn$. That is, $x^2 + 1$ is reducible if and only if there exist $m, n \in \{0, 1, \ldots, p - 1\}$ such that $p|(m + n)$ and $p|(mn - 1)$. Given the range of values for m and n, we can only have $m + n \in \{0, p\}$. But m and n cannot possibly both be 0, so $m + n = p$.

11.11 (1) The only possible rational roots are ± 1, ± 2. But none of these work, so it has no rational roots.

(2) The possible rational roots are of the form m/n, where $m|(-2)$ and $n|6$. Trying all of the possibilities, we see that $-1/2$ and $2/3$ are roots.

11.13 (1) Looking first for rational roots, we know that they must be integers and divide 18. We find that 3 is a root, so we have $(x-3)(x^3-7x^2+14x-6)$. Now, 3 is also a root of $x^3-7x^2+14x-6$, so we have $(x-3)^2(x^2-4x+2)$. By Eisenstein's criterion, we are now done.

(2) Looking first for rational roots, we see that they can only be ± 1, ± 2. In fact, -2 is a root, so we have $(x+2)(x^3+x+1)$. Now, the only possible rational roots of x^3+x+1 are 1 and -1, and these do not work. A degree 3 polynomial with no roots is irreducible, so we are done.

11.15 Note that $f(x)$ is a constant polynomial if and only if $f(x+a)$ is a constant polynomial. Thus, we may assume that both have degrees larger than 1. Suppose that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are nonconstant polynomials. Then $f(x+a) = g(x+a)h(x+a)$. As $g(x+a)$ and $h(x+a)$ are nonconstant polynomials, it follows that $f(x+a)$ is reducible. The converse is similar.

11.17 It is irreducible, using the preceding exercise with $p = 7$.

11.19 (1) We know that $2-3i$ must also be a root of $f(x)$, so $f(x)$ is divisible by $(x-(2+3i))(x-(2-3i)) = x^2-4x+13$. Performing the division, we get $f(x) = (x^2-4x+13)(x-7)$, so the third root is 7.

(2) Here, $1+i$ is also a root, so $f(x)$ is divisible by $(x-(1-i))(x-(1+i)) = x^2-2x+2$. Performing the division, we get $f(x) = (x^2-2x+2)(x^2+2x+3)$. By the quadratic equation, the remaining roots are $-1+\sqrt{2}i$ and $-1-\sqrt{2}i$.

11.21 (1) By Eisenstein's criterion, the polynomial is irreducible over $\mathbb{Q}$. In $\mathbb{R}[x]$, we can factor it as $(x-\sqrt[4]{10})(x+\sqrt[4]{10})(x^2+\sqrt{10})$. In $\mathbb{C}[x]$, we factor further and get $(x-\sqrt[4]{10})(x+\sqrt[4]{10})(x-\sqrt[4]{10}i)(x+\sqrt[4]{10}i)$.

(2) Using the Rational Roots Theorem, we find that 2 is a root. Thus, we can factor it as $(x-2)(x^2+3x+11)$. But $x^2+3x+11$ is irreducible over $\mathbb{R}$, hence over $\mathbb{Q}$, so we are done in those two cases. For $\mathbb{C}$, we use the quadratic equation and get $(x-2)(x-(-3+\sqrt{35}i)/2)(x-(-3-\sqrt{35}i)/2)$.

11.23 The roots must also include $2+5i$ and $4-i$, so we can use

$$\begin{aligned}&(x-(2-5i))(x-(2+5i))(x-(4+i))(x-(4-i))(x-6)\\ =&x^5-18x^4+150x^3-768x^2+2293x-2958.\end{aligned}$$

11.25 (1) Reducing modulo 5, we get x^3+2x+1. We see that it has no roots in $\mathbb{Z}_5$, and since it has degree 3, the polynomial is irreducible in $\mathbb{Z}_5[x]$, and hence $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(2) Reducing modulo 3, we get x^4+x^2+2. This has no roots in $\mathbb{Z}_3$, but we must rule out the possibility of a product of two polynomials of degree 2. We may assume

that both such polynomials are monic, and we can only have something of the form $(x^2 + ax + 1)(x^2 + bx + 2) = x^4 + x^2 + 2$. Comparing coefficients, we find that $a + b = 0$ and $2a + b = 0$. Thus, $a = b = 0$. But $(x^2 + 1)(x^2 + 2) = x^4 + 2 \neq x^4 + x^2 + 2$. Thus, our polynomial is irreducible in $\mathbb{Z}_3[x]$, and $f(x)$ is irreducible in $\mathbb{Q}[x]$.

11.27 The monic polynomials of degree 2 are precisely those of the form x^2+ax+b, with $a, b \in F$. There are thus n^2 of them. Such a polynomial is reducible if and only if it factors as $(x-c)(x-d)$, with $c, d \in F$. When $c = d$, there are n choices. If $c \neq d$, there are n choices for c and $n-1$ for d. Of course, $(x-c)(x-d) = (x-d)(x-c)$, so we get $n(n-1)/2$ possibilities, for a total of $n + n(n-1)/2 = n(n+1)/2$ reducible polynomials. By unique factorization, all of them are distinct. Thus, the number of irreducibles is $n^2 - n(n+1)/2 = n(n-1)/2$.

11.29 (1) $x^4 + 1 = (x^2 + a)(x^2 - a)$.
(2) $x^4 + 1 = (x^2 + ax - 1)(x^2 - ax - 1)$.
(3) $x^4 + 1 = (x^2 + ax + 1)(x^2 - ax + 1)$.

Problems of Chapter 12

12.1 No, as $x^n + 1$ and x^n lie in V but their difference, 1, does not.

12.3 We have $0 \in U$ and $0 \in W$, so $0 \in U \cap W$. If $v_1, v_2 \in U \cap W$, then $v_1, v_2 \in U$, so $v_1 + v_2 \in U$. Similarly, $v_1 + v_2 \in W$, so $v_1 + v_2 \in U \cap W$. If $a \in F$, then $av_1 \in U$ and $av_1 \in W$, so $av_1 \in U \cap W$. The argument for an arbitrary collection of subspaces is similar.

12.5 As $0 \in U$, we have $0 = \alpha(0) \in \alpha(U)$. (This follows immediately from the fact that α is, by definition, a homomorphism of additive groups.) Also, if $\alpha(u_1), \alpha(u_2) \in \alpha(U)$ and $a \in F$, then $\alpha(u_1) + \alpha(u_2) = \alpha(u_1 + u_2) \in \alpha(U)$, since $u_1 + u_2 \in U$, and $a\alpha(u_1) = \alpha(au_1) \in \alpha(U)$, since $au_1 \in U$.

12.7 It is. As $2 \cdot 0 + 3 \cdot 0 + 7 \cdot 0 = 0$, we see that $(0, 0, 0) \in W$. Suppose that $(a_1, b_1, c_1), (a_2, b_2, c_2) \in W$ and $a \in F$. Then $2(a_1+a_2)+3(b_1+b_2)+7(c_1+c_2) = (2a_1+3b_1+7c_1)+(2a_2+3b_2+7c_2) = 0+0 = 0$, so $(a_1+a_2, b_1+b_2, c_1+c_2) \in W$. Also, $2aa_1+3ab_1+7ac_1 = a(2a_1+3b_1+7c_1) = a \cdot 0 = 0$; thus, $(aa_1, ab_1, ac_1) \in W$.

12.9 We have $v + v + v = 1v + 1v + 1v = (1 + 1 + 1)v = 0v = 0$.

12.11 (1) As $3(1, 3, 5) + 2(2, 1, 4) - 1(7, 11, 23) = (0, 0, 0)$, they are linearly dependent.

(2) Suppose that $a(1, 3, 4)+b(2, 2, 1)+c(3, 6, 3) = (0, 0, 0)$. Then $a+2b+3c = 3a + 2b + 6c = 4a + b + 3c = 0$. Thus, $3a - b = a - 2b = 0$. We see immediately that $a = b = 0$, and hence $c = 0$. Therefore, the vectors are linearly independent.

12.13 (1) No. If they did, then as $(1,0,2)+(2,5,3)=(3,5,5)$, the vectors are linearly dependent, which means that some proper subset would form a basis for $\mathbb{Q}^3$. But $\mathbb{Q}^3$ is 3-dimensional over $\mathbb{Q}$, so this is impossible.

(2) Yes. We claim that the vectors are linearly independent. If $a(1,0,2)+b(2,3,5)+c(0,0,4)=(0,0,0)$, we see immediately that $b=0$, from which it follows that $a=0$ and then $c=0$. Thus, we can add vectors to this set to find a basis for $\mathbb{Q}^3$. But again, we are in a space with dimension 3, so no more vectors can be added. Therefore, the vectors span the space.

12.15 If the field is $\mathbb{C}$, we can see that every matrix can be written in a unique and obvious way as a linear combination of $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}$, so these matrices form a basis and the dimension is 4. Working over $\mathbb{R}$, we would also need $\begin{pmatrix}i&0\\0&0\end{pmatrix}, \begin{pmatrix}0&i\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\i&0\end{pmatrix}, \begin{pmatrix}0&0\\0&i\end{pmatrix}$, so the dimension is 8.

12.17 Let $\dim V=n$. If $n=0$, then $V=\{0\}$ and the only possible subspace is $\{0\}$, so there is nothing to do. So assume that $n\geq 1$. If $W=\{0\}$, then again, there is nothing to do. So assume that there exists $0\neq w_1\in W$. Then w_1 is, by itself, linearly independent. If w_1 spans W, then we have a basis for W. If not, then there exists a $w_2\in W$ such that w_2 is not a scalar multiple of w_1. But now w_1 and w_2 are linearly independent. If they span W, we have a basis. Otherwise, find $w_3\in W$ such that w_3 is not a linear combination of w_1 and w_2. Repeat this procedure. We cannot possibly go beyond w_n, as V cannot have $n+1$ linearly independent vectors. Thus, W has a basis consisting of at most n elements, so $\dim W\leq \dim V$. If $W\neq V$, then we can add to the basis for W to obtain a basis for V, which means we must have $\dim W<\dim V$.

12.19 Suppose that $a_1\alpha(v_1)+a_2\alpha(v_2)+\cdots+a_n\alpha(v_n)=0$, for some $a_i\in F$. Then $\alpha(a_1v_1+\cdots+a_nv_n)=0$. As α is one-to-one, $a_1v_1+\cdots+a_nv_n=0$. But the v_i are linearly independent. Thus, $a_1=\cdots=a_n=0$.

12.21 Let $a=\sqrt{5}+\sqrt{7}$. Then $a^2=12+2\sqrt{35}$, so $(a^2-12)^2=140$. Thus, a satisfies $f(x)=x^4-24x^2+4$. We must show that $f(x)$ is irreducible over $\mathbb{Q}$. If it has a root in $\mathbb{Q}$, then by the Rational Roots Theorem, the root must lie in $\{\pm1,\pm2,\pm4\}$. But none of these work. The only other possibility is that $f(x)$ is the product of two polynomials of degree 2. By Theorem 11.4, they may be assumed to be in $\mathbb{Z}[x]$. Up to a factor of -1, and noting that there is no x^3 term in $f(x)$, the factorization must be $(x^2+bx+c)(x^2-bx+d)$, for some $b,c,d\in\mathbb{Z}$. As there is no x term in $f(x)$, either $b=0$ or $c=d$. If $b=0$, we have $c+d=-24$ and $cd=4$. No integers can possibly satisfy these equations. So, assume that $c=d$. We are left with the cases $(x^2+bx+2)(x^2-bx+2)$ and $(x^2+bx-2)(x^2-bx-2)$, for some integer b. These possibilities yield, respectively, $4-b^2=-24$ and $-4-b^2=-24$. Neither of these equations has a solution in $\mathbb{Z}$.

12.23 Suppose that $[K:F]=n$. If $a\in K$, then $1,a,a^2,\ldots,a^n$ are linearly dependent over F, by Lemma 12.1. Thus, there exist $b_i\in F$, not all zero, such that $b_0+b_1a+b_2a^2+\cdots+b_na^n=0$. That is, a is a root of $b_0+b_1x+\cdots+b_nx^n$.

12.25 Let $L = \bigcup_{n=1}^{\infty} F_n$. As $1 \in F_1$, we have $1 \in L$. Suppose that $r, s \in L$. Then $r \in F_m$, $s \in F_n$, for some $m, n \in \mathbb{N}$. Letting k be the larger of m and n, we have $r, s \in F_k$. Thus, $r - s \in F_k \subseteq L$ and, if $s \neq 0$, $rs^{-1} \in F_k \subseteq L$.

12.27 As $a \in F(a)$ and $F(a)$ is a field, we must have $a^2 \in F(a)$. Also, $F \subseteq F(a)$. As $F(a^2)$ is the intersection of all subfields of K containing F and a^2, it follows that $F(a^2) \subseteq F(a)$. For the second part, let $F = \mathbb{Q}$ and $a = i$. Then $\mathbb{Q}(a^2) = \mathbb{Q}(-1) = \mathbb{Q}$, but $\mathbb{Q}(a)$ contains i, so the fields are different.

12.29 The minimal polynomial of a is irreducible over $\mathbb{C}$. By the Fundamental Theorem of Algebra, this minimal polynomial has degree 1, and must therefore be $x - a \in \mathbb{C}[x]$; thus, $a \in \mathbb{C}$.

12.31 Note that $f(x) = x^3 + x + 1$ is irreducible over $\mathbb{Z}_7$. (It has degree 3 and no roots in $\mathbb{Z}_7$.) Thus, $F = \mathbb{Z}_7[x]/(f(x))$ will work. Letting $a = x + (f(x))$, we know that the elements of F are the linear combinations of 1, a and a^2 over $\mathbb{Z}_7$. Also, a is a root of $f(x)$, so $a^3 = -a - 1 = 6a + 6$ and $a^4 = (6a + 6)a = 6a^2 + 6a$. Thus, $(a^2 + 5a + 4)(3a^2 + 6) = 3a^4 + a^3 + 4a^2 + 2a + 3 = 3(6a^2 + 6a) + (6a + 6) + 4a^2 + 2a + 3 = a^2 + 5a + 2$.

12.33 If a and b are any two roots of $x^3 - 2$, then $(ab^{-1})^3 = 1$, so ab^{-1} is one of the roots of $x^3 - 1$. One such root in $\mathbb{C}$ is 1 and another is ω. Also, $(\omega^2)^3 = 1$, so ω^2 is the third complex root of $x^3 - 1$. Thus, since $\mathbb{Q}(\sqrt[3]{2}, \omega)$ must contain $\sqrt[3]{2}$, 1, ω and ω^2, we see that it contains every root of $x^3 - 2$; in particular, $x^3 - 2$ splits over $\mathbb{Q}(\sqrt[3]{2}, \omega)$. On the other hand, if $x^3 - 2$ splits over any subfield, then that subfield would have to contain all three roots, namely, $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. As it is a field, this means it must contain ω as well, so it is all of $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

12.35 Note that $\mathbb{Q}(\sqrt{2})$ is a splitting field of $x^2 - 2$ over $\mathbb{Q}$. (Both roots, $\sqrt{2}$ and $-\sqrt{2}$ are in the field, and would have to be in any splitting field.) As an automorphism α must map the identity to the identity, we see immediately that $\alpha(c) = c$ for all $c \in \mathbb{Z}$. Similarly, if $m, n \in \mathbb{Z}$ with $n > 0$, then $m = \alpha(m) = \alpha(n(m/n)) = n\alpha(m/n)$. Thus, $\alpha(c) = c$ for all $c \in \mathbb{Q}$. By the preceding exercise, $\alpha(\sqrt{2})$ must be a root of $x^2 - 2$; in particular, $\alpha(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$. In the former case, α is the identity function. In the latter case, $\alpha(a + b\sqrt{2}) = a - b\sqrt{2}$ for all $a, b \in \mathbb{Q}$. By Lemma 12.4, this is an automorphism.

12.37 Let K be a splitting field for $f(x)$ over F. Say that in $K[x]$, we have $f(x) = a(x-a_1)(x-a_2)\cdots(x-a_n)$. Then $g(x) = a(x+1-a_1)(x+1-a_2)\cdots(x+1-a_n) = a(x - (a_1 - 1))(x - (a_2 - 1))\cdots(x - (a_n - 1))$. Since the a_i lie in K, so do the $a_i - 1$; thus, $g(x)$ splits over K. Furthermore, for $g(x)$ to split, all of the $a_i - 1$ must be present, and hence so must all of the a_i. Thus, we cannot make K any smaller and have $g(x)$ split, so K is a splitting field for $g(x)$. Showing that splitting fields for $g(x)$ must be splitting fields for $f(x)$ involves a similar argument.

12.39 If $|F| = p^n$, for some prime p and positive integer n, then F has one proper subfield for each integer m, $1 \leq m < n$, with $m|n$. The first value n that works is 6, so the smallest such field has order $2^6 = 64$. Specifically, it is the splitting field of $x^{64} - x$ over $\mathbb{Z}_2$.

12.41 Let $a \in K$ be a root of $f(x)$. Then $[\mathbb{Z}_5(a) : \mathbb{Z}_5] = 3$. If all roots of $f(x)$ lie in $\mathbb{Z}_5(a)$, then $K = \mathbb{Z}_5(a)$, and $|K| = 5^3$. Otherwise, in $\mathbb{Z}_5(a)[x]$, we have $f(x) = (x - a)g(x)$, where $g(x)$ is an irreducible polynomial of degree 2. Letting b be a root of $g(x)$ in K, we see that $[\mathbb{Z}_5(a, b) : \mathbb{Z}_5(a)] = 2$. Furthermore, in $\mathbb{Z}_5(a, b)$, the polynomial $f(x)$ splits into linear factors, so $K = \mathbb{Z}_5(a, b)$. Now, $[K : \mathbb{Z}_5] = [K : \mathbb{Z}_5(a)][\mathbb{Z}_5(a) : \mathbb{Z}_5] = 2 \cdot 3 = 6$, and $|K| = 5^6$.

12.43 Every field of characteristic 0 is perfect, so char $F = p$, for some prime p. The fact that $f(x) = a_0 + a_p x^p + \cdots + a_{mp} x^{mp}$ follows exactly as in the proof of Theorem 12.16. Suppose that all of the a_i are algebraic over the prime subfield, (an isomorphic copy of) $\mathbb{Z}_p$. Then $[\mathbb{Z}_p(a_0) : \mathbb{Z}_p] < \infty$. Also, a_p is algebraic over $\mathbb{Z}_p$, and hence over $\mathbb{Z}_p(a_0)$, so $[\mathbb{Z}_p(a_0, a_p) : \mathbb{Z}_p(a_0)] < \infty$. Thus, $[\mathbb{Z}_p(a_0, a_p) : \mathbb{Z}_p] = [\mathbb{Z}_p(a_0, a_p) : \mathbb{Z}_p(a_0)][\mathbb{Z}_p(a_0) : \mathbb{Z}_p] < \infty$. In the same way, $[\mathbb{Z}_p(a_0, a_p, \ldots, a_{mp} : \mathbb{Z}_p] < \infty$, which means that $\mathbb{Z}_p(a_0, a_p, \ldots, a_{mp})$ is a finite field, and hence perfect. If $f(x)$ is irreducible over F, it is surely irreducible over $\mathbb{Z}_p(a_0, \ldots, a_{mp})$. An irreducible polynomial over a perfect field cannot have multiple roots in any extension field.

12.45 If it were cyclic, it would be infinite cyclic. But note that $-1 \in U(F)$, and -1 has order 2. An infinite cyclic group has no such element.

12.47 Let F be the splitting field of $x^{125} - x$ over $\mathbb{Z}_5$. We know that it has order 125. Let $f(x) \in \mathbb{Z}_5[x]$ be an irreducible factor of $x^{125} - x$. If $a \in F$ is a root of $f(x)$, then $[\mathbb{Z}_5(a) : \mathbb{Z}_5] = \deg(f(x))$. But $\mathbb{Z}_5(a)$ is a subfield of F. A subfield of a field of order 5^3 can only have order 5 or 5^3. Thus, $\deg(f(x)) = 1$ or 3.

Problems of Chapter 13

13.1 WKHWUHDVXUHLVEXULHGWZHQWBSDFHVQRUWKRIWKHSDOPWUHH

13.3 We need k to be relatively prime to 26. If it is not, then letting $d = (26, k)$, we see that both 0 and $26/d$ will be encrypted as 0, so decryption will be impossible. On the other hand, if $(k, 26) = 1$, then $k \in U(26)$, so we can decrypt by multiplying by k^{-1}. (If $k \equiv 1 \pmod{26}$, then multiplying by k does not change the text at all, so it would be reasonable to rule out this key as well.)

13.5 JGVSHNEGJESCRPPRBSXBPPVGHBSJKEHXVT

13.7 KXTNRHIOQJHVKWNKSVNHSWOXCLFAAMJSKSBO

13.9 Writing $n = pq$, the smaller of p and q must certainly be less than $\sqrt{n}$, so we only need to try primes up to 44. We discover that $p = 37$ and $q = 53$. Thus, $\varphi(n) = 36 \cdot 52 = 1872$. To find d, we use the Euclidean algorithm. In particular, $1872 = 43(43) + 23$; $43 = 23(1) + 20$; $23 = 20(1) + 3$; $20 = 3(6) + 2$;

$3 = 2(1)+1; 2 = 1(2)+0$. Thus, $1 = 3(1)+2(-1) = 3(1)+(20(1)+3(-6))(-1) = 20(-1) + 3(7) = 20(-1) + (23(1) + 20(-1))(7) = 23(7) + 20(-8) = 23(7) + (43(1)+23(-1))(-8) = 43(-8)+23(15) = 43(-8)+(1872(1)+43(-43))(15) = 1872(15) + 43(-653)$. Therefore, $43(-653) \equiv 1 \pmod{1872}$. As we need d to be positive, adding 1872, we get $d = 1219$.

13.11 We must break our message into blocks of length 2. As we have an odd number of letters, we add a Q to the end. Then AL is 0011, GE is 0604, BR is 0117 and AQ is 0016. Next, $11^{149} \equiv 5581 \pmod{17399}$, $604^{149} \equiv 2315 \pmod{17399}$, $117^{149} \equiv 4926 \pmod{17399}$ and $16^{149} \equiv 9527 \pmod{17399}$, so our encrypted message consists of the four numbers 5581, 2315, 4926 and 9527.

13.13 Note that $n = 103 \cdot 179 = 18437$ and $\varphi(n) = 102 \cdot 178 = 18156$. To find d, we apply the Euclidean algorithm. Namely, $18156 = 151(120) + 36$; $151 = 36(4) + 7$; $36 = 7(5) + 1$; $7 = 1(7) + 0$. Thus, $1 = 36(1) + 7(-5) = 36(1) + (151(1) + 36(-4))(-5) = 151(-5) + 36(21) = 151(-5) + (18156(1) + 151(-120))(21) = 18156(21) + 151(-2525)$. Therefore, $-2525e \equiv 1 \pmod{\varphi(n)}$. As we need d to be positive, we add 18156 and get $d = 15631$. We now calculate $2469^{15631} \equiv 1514 \pmod{18437}$, $7093^{15631} \equiv 1124 \pmod{18437}$, $14773^{15631} \equiv 1314 \pmod{18437}$, $10900^{15631} \equiv 1208 \pmod{18437}$ and $143^{15631} \equiv 11 \pmod{18437}$ (which we remember to write as 0011). So, our message is 15141124131412080011, which translates to POLYNOMIAL.

Problems of Chapter 14

14.1 Construct the line through A and B. Next, construct the circle centred at A with radius AB. Say it meets the line at B and C. Construct the circle centred at B with radius AB, and say that it meets the line at A and E. Then the distance from C to E is 3, so if we construct the perpendicular bisector of CE, and it meets the line at D, then the distance from C to D is 1.5.

14.3 Construct the circle centred at A with radius AB and the circle centred at B with radius AB. Let C be either of the intersection points of these circles. By construction, the three sides of ABC have the same length.

14.5 We begin by constructing the line through B and A. Next, construct the circle centred at B with radius BC. It meets the line through B and A at two points; let E be the one of those points on the same side of B as A. Then replacing A with E, we may assume that in our original angle, A and C were equidistant from B. Construct the line through A and C, then construct the perpendicular bisector of AC. These two lines meet at the desired point, D.

14.7 Proceeding as in the solution to Exercise 14.3, construct a point E such that ABE is an equilateral triangle. It must lie on the circle. Now do the same thing with A and E; that is, construct a point C (the one that is different from B) such that AEC is an equilateral triangle. Again, C must be on the circle. Now do the same with A and C, and construct a new point F on the circle such that ACF is an equilateral triangle. Performing the same construction for A and F, we obtain a new point D on the circle such that AFD is an equilateral triangle. And then in the same way, we can construct a point G on the circle such that ADG is an equilateral triangle. But now $BECFDG$ is a regular hexagon, so BCD is an equilateral triangle.

14.9 As the constructible numbers form a field, if $a + b$ were constructible, then $a+b-a = b$ would also be constructible, giving a contradiction. Similarly, if ab were constructible, then the field of constructible numbers would include $a^{-1}ab = b$. Now, if $-b$ were constructible then b would be constructible as well, so letting $c = -b$, we see that $b + c = 0$ is constructible. On the other hand, if we let $c = b$, then we get $b + c = 2b$. If this were constructible, then since $1/2$ is also constructible, we would find that b would be constructible as well.

14.11 (1) Yes. As all integers are constructible and the field of constructible numbers is closed under the taking of square roots of its nonnegative elements, we see that $2 + \sqrt{5} - \sqrt{3}$ is constructible, and then we can take the square root twice to obtain this element.

(2) No. Once again, we know that $\sqrt{3}$ is constructible, but $\sqrt[3]{3}$ is a root of $x^3 - 3$. By Eisenstein's criterion, this polynomial is irreducible over $\mathbb{Q}$, so $\sqrt[3]{3}$ has minimal polynomial $x^3 - 3$. As the degree is not a power of 2, $\sqrt[3]{3}$ is not constructible. By Exercise 14.9, the sum of a number that is constructible with one that is not is not constructible.

14.13 By Eisenstein's criterion, this polynomial is irreducible over $\mathbb{Q}$. Thus, it is the minimal polynomial of a over $\mathbb{Q}$. As the degree is not a power of 2, a is not constructible.

14.15 We will prove a stronger statement, that an angle of $\pi/6$ can be constructed. We are given the points $(0, 0)$ and $(1, 0)$. To obtain such an angle, we only need to construct the point $(\cos(\pi/6), \sin(\pi/6)) = (\sqrt{3}/2, 1/2)$. But by Theorems 14.1 and 14.2, the numbers $\sqrt{3}/2$ and $1/2$ are constructible, so the point is constructible.

14.17 There is nothing to do for $n = 1$. When $n = 2$, we have $\cos(2\theta) = 2\cos^2(\theta) - 1$. For the $n = 3$ case, we look to the proof of Theorem 14.6, and see that $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$. To handle the remaining cases, we simply note that $\cos(\theta) = \cos(-\theta) = \cos(2\pi - \theta)$. Thus, $\cos(4\theta) = \cos(8\pi/7) = \cos(6\pi/7) = \cos(3\theta)$ and, similarly, $\cos(5\theta) = \cos(2\theta)$ and $\cos(6\theta) = \cos(\theta)$.

14.19 Let $D = A$. We know that the number $\sqrt{2}$ is constructible, which means that the point $E = (\sqrt{2}, 0)$ is constructible. Construct the circle centred at A and passing through C. It will meet the x-axis (which we can construct) at $(m, 0)$, where m is the distance from A to C. Thus, the number m is constructible, and so $m\sqrt{2}$ is constructible. In particular, we can construct the point $(m\sqrt{2}, 0)$. Now draw the circle centred at A and passing through $(m\sqrt{2}, 0)$. It intersects the line through A and C at a point F, where the distance from A to F is $m\sqrt{2}$ and F is on the same side of A as C. The triangles ABC and DEF are similar. As the side lengths are increased by a factor of $\sqrt{2}$, the area is increased by a factor of 2.

Index

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1