Lecture Notes on Groups and Rings

by Stephen New

Chapter 1. Definition and Examples of Groups and Subgroups

1.1 Definition: A **binary operation** on a set S is a function $*: S^2 \to S$, where

$$S^2 = S \times S = \{(a,b) \big| a, b \in S\} .$$

We usually write $a * b$ instead of $*(a,b)$.

1.2 Definition: A **group** is a set G together with a binary operation $*: G^2 \to G$ and an element $e = e_G \in G$ such that

(1) $*$ is *associative*: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
(2) e is an *identity* element: $a * e = e * a = a$ for all $a \in G$, and
(3) every $a \in G$ has an *inverse*: for all $a \in G$ there exists $b \in G$ such that $a * b = b * a = e$.

If, in addition, $*$ is *commutative*, that is $a * b = b * a$ for all $a, b \in G$, then we say that G is **abelian**.

1.3 Theorem: (*Uniqueness of the Identity*) *Let G be a group under $*$. For all $u, v \in G$, if $u * a = a$ for all $a \in G$ and $a * v = a$ for all $a \in G$ then $u = v$.*

Proof: Let $u, v \in G$. Suppose that $u * a = a$ for all $a \in G$ and $a * v = a$ for all $a \in G$. Since $u * a = a$ for all $a \in G$ we have $u * v = v$. Since $a * v = a$ for all $a \in G$ we have $u * v = u$. Thus $u = u * v = v$.

1.4 Theorem: (*Uniqueness of the Inverse*) *Let G be a group under $*$ with identity e, and let $a \in G$. Then for all $u, v \in G$, if $u * a = e$ and $a * v = e$ then $u = v$.*

Proof: Let $u, v \in G$. Suppose that $u * a = e$ and $a * v = e$. Then

$$u = u * e = u * (a * v) = (u * a) * v = e * v = v .$$

1.5 Notation: Let G be a group. If the operation in G is called *addition*, then we denote the operation by $+$ and we assume that it is commutative, we denote the (unique) identity in the group by 0, and we denote the (unique) inverse of a given point $a \in G$ by $-a$. For $a, b \in G$, we write $a - b = a + (-b)$. For $a \in G$ and $k \in \mathbf{Z}^+$ we write $ka = a + a + \cdots + a$ (with k terms in the sum), $0a = 0$, and $(-k)a = k(-a) = -a - a - \cdots - a$. With this notation, for all $a, b \in G$ and all $k, l \in \mathbf{Z}$ we have $(k+l)a = ka + la$, $(-k)a = -(ka) = k(-a)$, $-(-a) = a$ and $-(a+b) = -a - b = -b - a$. This notation is called **additive notation**, and any group G in which the operation is called addition, and is written using additive notation, is called an **additive group**. Additive groups are always assumed to be abelian.

1.6 Notation: When the operation $*$ of a group G is any operation other than addition (or when the operation is unspecified), we usually write $a * b$ simply as ab, we usually denote the (unique) identity element by e, 1 or I, and we denote the (unique) inverse of $a \in G$ by a^{-1}. For $a \in G$ and $k \in \mathbf{Z}^+$ we write $a^k = aa \cdots a$ (with k terms in the product), $a^0 = e$, and $a^{-k} = (a^{-1})^k = a^{-1}a^{-1} \cdots a^{-1}$. With this notation, for all $a, b \in G$ and all $k, l \in \mathbf{Z}$ we have $a^{k+l} = a^k a^l$, $a^{-k} = (a^k)^{-1} = (a^{-1})^k$, $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$. The above notation is called **multiplicative notation**, and any group G in which the operation is written using multiplicative notation is called a **multiplicative group**.

1.7 Note: From now on, we shall use multiplicative notation as our default notation, unless the operation is known to be addition.

1.8 Theorem: (Cancellation) *Let G be a group with identity e. Let $a, b, c \in G$. Then*
(1) if $ab = ac$ or if $ba = ca$ then $b = c$.
(2) if $ab = e$ then $a^{-1} = b$ and $b^{-1} = a$.
(3) if $ab = a$ or if $ba = a$ then $b = e$.

Proof: To prove (1) note that if $ab = ac$ then multiplying both sides on the left by a^{-1} gives $b = c$; in greater detail, we have

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c\,.$$

Similarly, if $ba = ca$ then multiplying on the right by a^{-1} gives $b = c$. To prove part (2) note that if $ab = e$ then multiplying both sides on the left by a^{-1} gives $b = a^{-1}$, and multiplying on the right by b^{-1} gives $a = b^{-1}$. To prove part (3), note that if $ab = a$ then multiplying on the left by a^{-1} gives $b = e$, and if $ba = a$ then multiplying on the right by a^{-1} gives $b = e$.

1.9 Example: If R is a *ring* (as defined later) under the operations $+$ and $\cdot$, then R is also an abelian group under $+$ with identity 0. For example, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{H}$ and $\mathbf{Z}_n$ are abelian groups under $+$ with identity 0.

1.10 Example: If R is a ring under $\cdot$ with identity 1 (as defined later) then the set of units

$$R^* = \left\{a \in R \,\middle|\, a \text{ has an inverse under } \cdot\right\}$$

is a group under $\cdot$ with identity 1. For example, $\mathbf{Z}^* = \{\pm 1\}$, $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$, $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$, $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$, $\mathbf{H}^* = \mathbf{H} \setminus \{0\}$ and

$$U_n = {\mathbf{Z}_n}^* = \left\{a \in \mathbf{Z}_n \,\middle|\, \gcd(a, n) = 1\right\}$$

are abelian groups under multiplication with identity 1.

1.11 Example: If S is a set and G is a group, then the set of functions

$$\text{Func}(S, G) = G^S = \left\{f : S \to G\right\}$$

is a group under the operation given by $(fg)(x) = f(x)g(x)$ for all $x \in S$.

1.12 Example: For a set S, the set of permutations

$$\text{Perm}(S) = \left\{f : S \to S \,\middle|\, f \text{ is bijective}\right\}$$

is a group under composition with identity $I : S \to S$ given by $I(x) = x$ for all $x \in S$. This group is non-abelian when $|S| \geq 3$. For $n \in \mathbf{Z}^+$, the n^{th} **symmetric group** is the group

$$S_n = \text{Perm}\big(\{1, 2, \cdots, n\}\big)\,.$$

1.13 Example: When R is a commutative ring with identity, the set $M_n(R)$ of $n \times n$ matrices with entries in R is an abelian group under matrix addition with identity 0, and the **general linear group**

$$GL_n(R) = M_n(R)^* = \left\{A \in M_n(R) \,\middle|\, \det(A) \in R^*\right\}$$

is a group under matrix multiplication with identity I. This group is non-abelian for $n \geq 2$.

1.14 Example: If G and H are groups with identities e_G and e_H, then the **product**

$$G \times H = \{(a,b) \big| a \in G, b \in H\}$$

is a group under the operation given by $(a,b)(c,d) = (ac, bd)$ with identity (e_G, e_H). More generally, if $G_1, G_2, \cdots, G_n$ are groups then the direct product

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n = \{(a_1, a_2, \cdots, a_n) \big| a_i \in G_i\}$$

is a group under the operation $(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$. For a group G, we write $G^n = \prod_{i=1}^{n} G = G \times G \times \cdots \times G$. More generally still, if A is any set (possibly infinite) and G_α is a group for each $\alpha \in A$ the the direct product

$$\prod_{\alpha \in A} G_\alpha = \left\{ f : A \to \bigcup_{\alpha \in A} G_\alpha \middle| f(\alpha) \in G_\alpha \text{ for all } \alpha \in A \right\}$$

is a group with operation $(fg)(\alpha) = f(\alpha)g(\alpha) \in G_\alpha$ for all $\alpha \in A$. The **direct sum**

$$\sum_{\alpha \in A} G_\alpha = \left\{ f \in \prod_{\alpha \in A} G_\alpha \middle| f(\alpha) = e_\alpha \text{ for all but finitely many } \alpha \in A \right\}$$

where e_α is the identity in G_α, is also a group under the same operation $(fg)(x) = f(x)g(x)$.

1.15 Definition: For a finite group G, we can specify its operation $*$ by making a table showing the value of the product $a * b$ for each pair $(a,b) \in G^2$. Such a table is called an **operation table** (or an addition, multiplication or composition table) for G.

1.16 Example: The multiplication table for the group $U_{12} = \{1, 5, 7, 11\}$ is shown below.

$a \backslash b$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

1.17 Definition: Let G be a group and let $a \in G$. The **order** of G is its cardinality $|G|$. The **order** of a in G, denoted by $|a|$ or by $\text{ord}_G(a)$, is the smallest positive integer n such that $a^n = e$ (or in additive notation, the smallest positive integer n such that $na = 0$), provided that such an integer exists. If no such positive integer n exists, then the order of a is infinite.

1.18 Example: The order of $\mathbf{Z}_n$ is $\big|\mathbf{Z}_n\big| = n$. The order of $a \in \mathbf{Z}_n$ is $|a| = \frac{n}{\gcd(a,n)}$. Indeed if we let $d = \gcd(a,n)$ and write $a = sd$ and $n = td$, then $\gcd(s,t) = 1$ and we have $ka = 0 \in \mathbf{Z}_n \iff n | ka \iff td | ksd \iff t | ks \iff t | k$ and so $|a| = t = \frac{n}{d}$.

1.19 Example: The order of U_n is $|U_n| = \phi(n)$ where ϕ is the Euler phi function. We shall see later (in Corollary 4.22) that if $n = \prod {p_i}^{k_i}$ is the prime factorization of n then $\phi(n) = \prod ({p_i}^{k_i} - {p_i}^{k_i - 1}) = n \cdot \prod \left(1 - \frac{1}{p_i}\right)$.

1.20 Example: The order of the group $\mathbf{C}^*$ is $|\mathbf{C}^*| = \infty$ (or more accurately $|\mathbf{C}^*| = 2^{\aleph_0}$). For $a = re^{i\theta} \in \mathbf{C}^*$ where $r, \theta \in \mathbf{R}$ with $r > 0$, when $r \neq 1$ or when θ is not a rational multiple of 2π we have $|a| = \infty$, and when $r = 1$ and $\theta = \frac{2\pi k}{n}$ with $k, n \in \mathbf{Z}$ and $n \neq 0$ we have $|a| = \frac{n}{\gcd(k,n)}$.

1.21 Example: If S is a set and G is a group then $\big|\text{Func}(S,G)\big| = |G|^{|S|}$.

1.22 Example: If S is a finite set then $\big|\text{Perm}(S)\big| = |S|!$. In particular $|S_n| = n!$.

1.23 Example: When p is prime (so that $\mathbf{Z}_p$ is a *field*, as defined later), we have

$$\big|GL_n(\mathbf{Z}_p)\big| = (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1})\,.$$

Indeed, for a matrix $A \in M_n(\mathbf{Z}_p)$, in order for A to be invertible its columns must be linearly independent. The first column u_1 of A can be any non-zero vector in ${\mathbf{Z}_p}^n$ so there are $p^n - 1$ choices for u_1. Having chosen u_1, the second column u_2 can be any vector in ${\mathbf{Z}_p}^n$ which is not a multiple $t_1 u_1$, $t_1 \in \mathbf{Z}_p$. Since there are p such multiples, there are $p^n - p$ choices for the u_2. Having chosen u_1 and u_2, the third column u_3 can be any vector in ${\mathbf{Z}_p}^n$ which is not a linear combination $t_1u_1 + t_2u_2$, $t_1, t_2 \in \mathbf{Z}_p$. There are p^2 such linear combinations, so there are $p^n - p^2$ choices for u_3. And so on.

1.24 Example: If G and H are groups then $\big|G \times H\big| = |G|\,|H|$. For $a \in G$ and $b \in H$,

$$\big|(a,b)\big| = \text{lcm}\big(|a|,|b|\big)\,.$$

Indeed if $|a| = n$ and $|b| = m$ then for $k \in \mathbf{Z}$ we have

$$\begin{aligned}
(a,b)^k = e_{G\times H} &\iff (a^k, b^k) = (e_G, e_H) \\
&\iff \big(a^k = e_G \text{ and } b^k = e_H\big) \\
&\iff n\big|k \text{ and } m\big|k\big) \\
&\iff \ k \text{ is a common multiple of } n \text{ and } m.
\end{aligned}$$

1.25 Definition: Let G be a group. For $a, b \in G$, we say that a and b are **conjugate** in G, and we write $a \sim b$, when $b = xax^{-1}$ for some $x \in G$. For $a \in G$, we define the **conjugacy class** of a in G to be the set

$$Cl(a) = Cl_G(a) = \big\{b \in G \big| b \sim a\big\} = \big\{xax^{-1}\big| x \in G\big\}\,.$$

1.26 Note: The relation $\sim$ is an **equivalence relation** on G. This means that for all $a, b, c \in G$ we have

(1) $a \sim a$,
(2) if $a \sim b$ then $b \sim a$, and
(3) if $a \sim b$ and $b \sim c$ then $a \sim c$.

Indeed, given $a, b, c \in G$ we have $a \sim a$ since $a = eae^{-1}$, and if $a \sim b$, say $b = xax^{-1}$, then $a = x^{-1}b\,(x^{-1})^{-1}$ so $b \sim a$, and finally if $a \sim b$ and $b \sim c$ with say $b = xax^{-1}$ and $c = yby^{-1}$, then we have $c = yxay^{-1}x^{-1} = (yx)a(yx)^{-1}$ so $a \sim c$. It follows that G is the disjoint union of the distinct conjugacy classes.

1.27 Example: As an exercise, show that if $a \sim b$ in G, then $|a| = |b|$.

1.28 Definition: A **subgroup** of a group G is a subset $H \subseteq G$ which is also a group using the same operation as in G. When H is a subgroup of G, we write $H \leq G$.

1.29 Example: In any group G we have the subgroups $\{e\} \leq G$ and $G \leq G$. The group $\{e\}$ is called the **trivial** group. A subgroup $H \leq G$ with $H \neq G$ is called a **proper** subgroup of G.

1.30 Example: We have $\mathbf{Z} \leq \mathbf{Q} \leq \mathbf{R} \leq \mathbf{C} \leq \mathbf{H}$. and we have $\mathbf{Z}^* \leq \mathbf{Q}^* \leq \mathbf{R}^* \leq \mathbf{C}^* \leq \mathbf{H}^*$.

1.31 Example: Note that $\mathbf{Z}_n = \{0, 1, \cdots, n-1\}$ is not a subgroup of $\mathbf{Z}$, indeed it is not even a subset. Also, U_n is not a subgroup of $\mathbf{Z}_n$ since it uses a different operation.

1.32 Theorem: (*The Subgroup Test I) Let G be a group and let $H \subseteq G$. Then $H \leq G$ if and only if*

(1) H contains the identity, that is $e \in H$,
(2) H is closed under the operation, that is $ab \in H$ for all $a, b \in H$, and
(3) H is closed under inversion, that is $a^{-1} \in H$ for all $a \in H$.

Proof: Note first that the operation on the group G restricts to a well defined operation on H if and only if H is closed under the operation. In this case, the operation will be associative on H since it is associative on G. Next note that if $e = e_G \in H$ then e is an identity element for H, and conversely if e_H is an identity for H then since $e_H e_H = e_H$ (both in H and in G), cancellation in the group G gives $e_H = e_G$. Thus H has an identity if and only if $e = e_G \in H$. A similar argument shows that a given element $a \in H$ has an inverse in H if and only if $a^{-1} \in H$ where a^{-1} denotes the inverse of a in G.

1.33 Theorem: (*The Subgroup Test II) Let G be a group and let $H \subseteq G$. Then $H \leq G$ if and only if*

(1) $H \neq \emptyset$, and
(2) for all $a, b \in H$ we have $ab^{-1} \in H$.

Proof: From the Subgroup Test I, it is clear that if $H \leq G$ then (1) and (2) hold. Suppose, conversely, that (1) and (2) hold. By (1) we can choose an element $a \in H$, and then by (2) we have $e = aa^{-1} \in H$, so H contains the identity. For $a \in H$, we have $a^{-1} = ea^{-1} \in H$ by (2), so H is closed under inversion. For $a, b \in H$, we have $ab = a(b^{-1})^{-1} \in H$, so H is closed under the operation.

1.34 Theorem: (*The Finite Subgroup Test) Let G be a group and let H be a finite subset of H. Then $H \leq G$ if and only if*

(1) $H \neq \emptyset$, and
(2) H is closed under the operation, that is $ab \in H$ for all $a, b \in H$.

Proof: The proof is left as an exercise.

1.35 Example: The set $\{(x, y) \in \mathbf{R}^2 \big| xy \geq 0\}$ is not a subgroup of $\mathbf{R}^2$ since it is not closed under addition.

1.36 Example: For $n \in \mathbf{Z}^+$ we have $\mathbf{C}_n \leq \mathbf{C}_\infty \leq \mathbf{S}^1 \leq \mathbf{C}^*$ where

$$\mathbf{C}_n = \{z \in \mathbf{C}^* \big| z^n = 1\}$$
$$\mathbf{C}_\infty = \{z \in \mathbf{C}^* \big| z^n = 1 \text{ for some } n \in \mathbf{Z}^+\}$$
$$\mathbf{S}^1 = \{z \in \mathbf{C}^* \big| ||z|| = 1\}$$

1.37 Example: When R is a commutative ring with 1, in the general linear group $GL_n(R)$ we have the following subgroups, called the **special linear group**, the **orthogonal group** and the **special orthogonal group**.

$$\begin{aligned} SL_n(R) &= \left\{A \in M_n(R) \,\middle|\, \det(A) = 1\right\} \\ O_n(R) &= \left\{A \in M_n(R) \,\middle|\, A^t A = I\right\} \\ SO_n(R) &= \left\{A \in M_n(R) \,\middle|\, A^t A = I, \det(A) = 1\right\} \end{aligned}$$

1.38 Example: For $\theta \in \mathbf{R}$, the **rotation** in $\mathbf{R}^2$ about $(0,0)$ by the angle θ is given by the matrix

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

and the **reflection** in $\mathbf{R}^2$ in the line through $(0,0)$ and the point $\left(\cos\frac{\theta}{2}, \sin\frac{\theta}{2}\right)$ is given by the matrix

$$F_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

We have

$$\begin{aligned} O_2(\mathbf{R}) &= \left\{R_\theta, F_\theta \,\middle|\, \theta \in \mathbf{R}\right\} \\ SO_2(\mathbf{R}) &= \left\{R_\theta \,\middle|\, \theta \in \mathbf{R}\right\} \end{aligned}$$

In $O_2(\mathbf{R})$, for $\alpha, \beta \in \mathbf{R}$ we have

$$F_\beta F_\alpha = R_{\beta-\alpha}\ ,\ F_\beta R_\alpha = F_{\beta-\alpha}\ ,\ R_\beta F_\alpha = F_{\alpha+\beta}\ ,\ R_\beta R_\alpha = R_{\alpha+\beta}\,.$$

1.39 Example: For $n \in \mathbf{Z}^+$, the **dihedral group** D_n is the group

$$D_n = \left\{R_k, F_k \,\middle|\, k \in \mathbf{Z}_n\right\} = \left\{R_0, R_1, \cdots, R_{n-1}, F_0, F_1, \cdots F_{n-1}\right\}$$

where for $k \in \mathbf{Z}_n$ we write $R_k = R_{\theta_k}$ and $F_k = F_{\theta_k}$ with $\theta_k = \frac{2\pi k}{n}$. We have

$$D_n \le O_2(\mathbf{R}) \le GL_2(\mathbf{R}) \le \mathrm{Perm}(\mathbf{R}^2)$$

and for $k, l \in \mathbf{Z}_n$, the operation in D_n is given by

$$F_l F_k = R_{l-k}\ ,\ F_l R_k = F_{l-k}\ ,\ R_l F_k = F_{k+l}\ ,\ R_l R_k = R_{k+l}\,.$$

1.40 Definition: Let G be a group and let $a \in G$. The **centre** of G is the set

$$Z(G) = \left\{a \in G \,\middle|\, ax = xa \text{ for all } x \in G\right\}$$

and the **centralizer** of a in G is the set

$$C(a) = C_G(a) = \left\{x \in G \,\middle|\, ax = xa\right\}.$$

As an exercise, show that $Z(G)$ and $C_a(G)$ are both subgroups of G.

1.41 Example: Find the centre of D_4 and find the centralizers of R_k and F_k in D_4.

.

Chapter 2. Cyclic Groups and Generators

2.1 Example: If H and K are subgroups of G then so is $H \cap K$. More generally, if A is a set and $H_\alpha \leq G$ for each $\alpha \in A$, then $\bigcap\limits_{\alpha \in A} H_\alpha \leq G$ by the Subgroup Test II. Indeed we have $e_G \in H_\alpha$ for all $\alpha \in A$ so that $e_G \in \bigcap_{\alpha \in A} H_\alpha$, and if $a, b \in \bigcap\limits_{\alpha \in A} H_\alpha$ then for every $\alpha \in A$ we have $a, b \in H_\alpha$ hence $ab^{-1} \in H_\alpha$, and so $ab^{-1} \in \bigcap\limits_{\alpha \in A} H_\alpha$.

2.2 Definition: Let G be a group and let $S \subseteq G$. The **subgroup of** G **generated by** S, denoted by $\langle S \rangle$, is the smallest subgroup of G which contains S, that is the intersection of all subgroups of G which contain S. The elements of S are called **generators** of the group $\langle S \rangle$. When S is a finite set, we omit set brackets and write $\langle a_1, a_2, \cdots, a_n \rangle = \big\langle \{a_1, a_2, \cdots, a_n\} \big\rangle$. We say that G is **finitely generated** when $G = \langle S \rangle$ for some finite set $S \subseteq G$. We say that G is **cyclic** when $G = \langle a \rangle$ for some $a \in G$. When G is any group and $a \in G$, the group $\langle a \rangle$ is called the **cyclic subgroup of** G **generated by** a.

2.3 Theorem: *(Elements of a Cyclic Group) Let G be a group and let $a \in G$. Then*
(1) we have $\langle a \rangle = \big\{ a^k \big| k \in \mathbf{Z} \big\}$.
(2) If $|a| = \infty$ then the elements $a^k, k \in \mathbf{Z}$ are all distinct so we have $\big|\langle a \rangle\big| = \infty$.
(3) If $|a| = n$ then for $k, l \in \mathbf{Z}$ we have $a^k = a^l \iff k = l \bmod n$ and so

$$\langle a \rangle = \big\{ a^k \big| k \in \mathbf{Z}_n \big\} = \big\{ e, a, a^2, \cdots, a^{n-1} \big\}$$

with the listed elements in the above set all distinct so that $\big|\langle a \rangle\big| = n$. In particular, for $k \in \mathbf{Z}$ we have $a^k = e \iff n \big| k$.

Proof: First we show that $\langle a \rangle = \big\{ a^k \big| k \in \mathbf{Z} \big\}$. By definition, $\langle a \rangle$ is the intersection of all subgroups $H \leq G$ with $a \in H$. By closure under the operation and under inversion, if $H \leq G$ with $a \in H$ then $a^k \in H$ for all $k \in \mathbf{Z}$, and so $\big\{ a^k \big| k \in \mathbf{Z} \big\} \subseteq \langle a \rangle$. On the other hand, since $e = a^0$ and $a^k (a^l)^{-1} = a^{k-l}$, we see that $\big\{ a^k \big| k \in \mathbf{Z} \big\} \leq G$ by the Subgroup Test. Since $\big\{ a^k \big| k \in \mathbf{Z} \big\} \leq G$ and $a = a^1 \in \big\{ a^k \big| k \in \mathbf{Z} \big\}$, it follows that $\langle a \rangle \subseteq \big\{ a^k \big| k \in \mathbf{Z} \big\}$.

Now suppose that $|a| = \infty$ and suppose, for a contradiction, that $a^k = a^l$ with $k < l$. Then $a^{l-k} = a^l (a^k)^{-1} = a^l (a^l)^{-1} = e$ but this contradicts the fact that $|a| = \infty$.

Next suppose that $|a| = n$. Suppose that $a^k = a^l$. Then, as above, $a^{l-k} = e$. Write $l - k = qn + r$ with $0 \leq r < n$. Then $e = a^{l-k} = a^{qn+r} = (a^n)^q a^r = a^r$. Since $|a| = n$ we must have $r = 0$. Thus $l - k = qn$, that is $k = l \bmod n$. Conversely, suppose that $k = l \bmod n$, say $k = l + qn$. Then $a^k = a^{l+qn} = a^l (a^n)^q = a^l$.

2.4 Notation: When G is an abelian group under $+$, we have $\langle a \rangle = \{ka | k \in \mathbf{Z}\}$.

2.5 Example: The groups $\mathbf{Z}$ and $\mathbf{Z}_n$ are cyclic with $\mathbf{Z} = \langle 1 \rangle$ and $\mathbf{Z}_n = \langle 1 \rangle$. The group $\mathbf{C}_n = \{z \in \mathbf{C}^* | z^n = 1\}$ is cyclic with $\mathbf{C}_n = \big\langle e^{i\,2\pi/n} \big\rangle$.

2.6 Example: In the group $\mathbf{Z}$ we have $\langle 2 \rangle = \{\cdots, -2, 0, 2, 4, \cdots\}$, but in the group $\mathbf{R}^*$ we have $\langle 2 \rangle = \big\{ \cdots \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \cdots \big\}$.

2.7 Example: The group $U_{18} = \{1, 5, 7, 11, 13, 17\}$ is cyclic with $U_{18} = \langle 5 \rangle$ because in U_{18} we have

k	0	1	2	3	4	5
5^k	1	5	7	17	13	11

2.8 Theorem: (*The Classification of Subgroups of a Cyclic Group*) *Let G be group and let $a \in G$. Then*

(1) every subgroup of $\langle a \rangle$ is cyclic.

(2) If $|a| = \infty$ then $\langle a^k \rangle = \langle a^l \rangle \iff l = \pm k$ so the distinct subgroups of $\langle a \rangle$ are the trivial group $\langle a^0 \rangle = \{e\}$ and the groups $\langle a^d \rangle = \left\{ a^{kd} \middle| k \in \mathbf{Z} \right\}$ where $d \in \mathbf{Z}^+$.

(3) If $|a| = n$ then we have $\langle a^k \rangle = \langle a^l \rangle \iff \gcd(k,n) = \gcd(l,n)$ and so the distinct subgroups of $\langle a \rangle$ are the groups $\langle a^d \rangle = \left\{ a^{kd} \middle| k \in \mathbf{Z}_{n/d} \right\} = \left\{ a^0, a^d, a^{2d}, \cdots, a^{n-d} \right\}$ where d is a positive divisor of n.

Proof: First we show that every subgroup of $\langle a \rangle$ is cyclic. Let $H \leq \langle a \rangle$. If $H = \{e\}$ then $H = \langle e \rangle$, which is cyclic. Suppose that $H \neq \{e\}$. Note that H contains some element of the form a^k with $k \in \mathbf{Z}^+$ since we can choose $a^l \in H$ for some $l \neq 0$, and if $l < 0$ then we also have $a^{-l} = (a_l)^{-1} \in H$. Let k be the smallest positive integer such that $a^k \in H$. We claim that $H = \langle a^k \rangle$. Since $a^k \in H$, by closure under the operation and under inversion we have $(a^k)^i \in H$ for all $i \in \mathbf{Z}$ and so $\langle a^k \rangle \subseteq H$. Let $a^l \in H$, where $l \in \mathbf{Z}$. Write $l = kq + r$ with $0 \leq r < k$. Then $a^l = a^{kq} a^r$ so we have $a^r = a^l (a^{kq})^{-1} \in H$. By our choice of k we must have $r = 0$, so $l = qk$ and so $a^l \in \langle a^k \rangle$. Thus $H \subseteq \langle a^k \rangle$.

Suppose that $|a| = \infty$. If $l = \pm k$ then clearly $\langle a^l \rangle = \langle a^k \rangle$. Suppose that $\langle a^l \rangle = \langle a^k \rangle$. Since $a^k \in \langle a^l \rangle$ we have $l = kt$ for some $t \in \mathbf{Z}$, so $k \big| l$. Since $a^k \in \langle a^l \rangle$ we have $l \big| k$. Since $k \big| l$ and $l \big| k$ we have $l = \pm k$.

Now suppose that $|a| = n$. Note first that for any divisor $d \big| n$ we have

$$\langle a^d \rangle = \left\{ a^{dk} \middle| k \in \mathbf{Z}_{n/d} \right\} = \left\{ a^0, a^d, a^{2d}, \cdots, a^{n-d} \right\}$$

with the listed elements distinct so that $|a^d| = \frac{n}{d}$. We claim that $\langle a^k \rangle = \langle a^d \rangle$ where $d = \gcd(k,n)$. Since $d \big| k$ we have $a^k \in \langle a^d \rangle$ so $\langle a^k \rangle \subseteq \langle a^d \rangle$. Choose $s, t \in \mathbf{Z}$ so that $ks + nt = d$. Then $a^d = a^{ks+nt} = (a^k)^s (a^n)^t = (a^k)^s \in \langle a^k \rangle$ and so $\langle a^d \rangle \subseteq \langle a^k \rangle$. Thus $\langle a^k \rangle = \langle a^d \rangle$, as claimed. Now if $\langle a^k \rangle = \langle a^l \rangle$ and $d = \gcd(k,n)$ and $c = \gcd(l,n)$ then $\langle a^d \rangle = \langle a^k \rangle = \langle a^l \rangle = \langle a^c \rangle$ and so $\left| \langle a^d \rangle \right| = \left| \langle a^c \rangle \right|$, that is $\frac{n}{d} = \frac{n}{c}$, and so $d = c$. Conversely, if $d = \gcd(k,n) = \gcd(l,n) = c$ then we have $\langle a^k \rangle = \langle a^d \rangle = \langle a^l \rangle$.

2.9 Corollary: (*Orders of Elements in a Cyclic Group*) *Let G be a group and let $a \in G$.*
(1) If $|a| = \infty$ then $|a^0| = 1$ and $a^k = \infty$ for all $0 \neq k \in \mathbf{Z}$, and
(2) if $|a| = n$ then $|a^k| = \frac{n}{\gcd(k,n)}$ for all $k \in \mathbf{Z}$.

2.10 Corollary: (*Generators of a Cyclic Group*) *Let G be a group and let $a \in G$. Then*
(1) if $|a| = \infty$ then $\langle a^k \rangle = \langle a \rangle \iff k = \pm 1$, and
(2) if $|a| = n$ then $\langle a^k \rangle = \langle a \rangle \iff \gcd(k,n) = 1 \iff k \in U_n$.

2.11 Corollary: (*The Number of Elements of Each Order in a Cyclic Group*) *Let G be a group and let $a \in G$ with $|a| = n$. Then for each $k \in \mathbf{Z}$, the order of a^k is a positive divisor of n, and for each positive divisor $d \big| n$, the number of elements in $\langle a \rangle$ of order d is equal to $\phi(d)$.*

2.12 Corollary: *For $n \in \mathbf{Z}^+$ we have* $\sum_{d|n} \phi(d) = n$.

2.13 Corollary: (*The Number of Elements of Each Order in a Finite Group*) *Let G be a finite group. For each $d \in \mathbf{Z}^+$, the number of elements in G of order d is equal to $\phi(d)$ multiplied by the number of cyclic subgroups of G of order d.*

2.14 Theorem: (*Elements of $\langle S \rangle$*) *Let G be a group and let $\emptyset \neq S \subseteq G$. Then*

$$\begin{aligned}\langle S \rangle &= \left\{ {a_1}^{k_1} {a_2}^{k_2} \cdots {a_l}^{k_l} \middle| l \geq 0, a_i \in S, k_i \in \mathbf{Z} \right\} \\ &= \left\{ {a_1}^{k_1} {a_2}^{k_2} \cdots {a_l}^{k_l} \middle| l \geq 0, a_i \in S \text{ with } a_i \neq a_{i+1}, 0 \neq k_i \in \mathbf{Z} \right\}\end{aligned}$$

where the empty product (when $l = 0$) is the identity element. If G is abelian then

$$\langle S \rangle = \left\{ {a_1}^{k_1} {a_2}^{k_2} \cdots {a_l}^{k_l} \middle| l \geq 0, a_i \in S \text{ with } a_i \neq a_j \text{ for } i \neq j, 0 \neq k_i \in \mathbf{Z} \right\}.$$

Proof: The proof is left as an exercise.

2.15 Notation: If G is an additive abelian group then

$$\langle S \rangle = \text{Span}_{\mathbf{Z}}\{S\} = \left\{ k_1 a_1 + k_2 a_2 + \cdots + k_l a_l \middle| l \geq 0, a_i \in S, a_i \neq a_j \text{ for } i \neq j, 0 \neq k_i \in \mathbf{Z} \right\}.$$

2.16 Example: As an exercise, show that in $\mathbf{Z}$ we have $\langle k, l \rangle = \langle d \rangle$ where $d = \gcd(k, l)$.

2.17 Example: In $\mathbf{Z}^2$, the elements of $\big\langle (1,3), (2,1) \big\rangle$ are the vertices of parallelograms which cover $\mathbf{R}^2$.

2.18 Example: We have $D_n = \big\langle R_1, F_0 \big\rangle \leq O_2(\mathbf{R})$ because $R_k = {R_1}^k$ and $F_k = R_k F_0$.

2.19 Definition: Let S be a set. The **free group** on S is the set whose elements are

$$F(S) = \left\{ {a_1}^{k_1} {a_2}^{k_2} \cdots {a_l}^{k_l} \middle| l \geq 0, a_i \in S, 0 \neq k_i \in \mathbf{Z} \right\}$$

with the operation given by concatenation

$$({a_1}^{j_1} \cdots {a_l}^{j_l})({b_1}^{k_1} \cdots {b_m}^{k_m}) = {a_1}^{j_1} \cdots {a_l}^{j_l} {b_1}^{k_1} \cdots {b_m}^{k_m}$$

followed by grouping and cancellation in the sense that if $a_l = b_1$ then we replace ${a_l}^{j_l} {b_1}^{k_1}$ by ${a_l}^{j_l + k_1}$ and if, in addition, $j_l + k_1 = 0$ then we omit the term ${a_l}^0$ and perform further grouping if $a_{l-1} = b_2$. For example, in $F(a, b)$ we have

$$(a\,b^2 a^{-3} b)(b^{-1} a^3 b\,a^{-2}) = a\,b^2 a^{-3} b\,b^{-1} a^3 b\,a^{-2} = a\,b^2 a^{-3} a^3 b\,a^{-2} = a\,b^2 b\,a^{-2} = a\,b^3 a^{-2}.$$

Note that in the free group $F(S)$ we have $F(S) = \langle S \rangle$.

2.20 Definition: Let S be a set. The **free abelian group** on S is the set

$$A(S) = \left\{ k_1 a_1 + \cdots + k_l a_l \middle| l \geq 0, a_i \in S \text{ with } a_i \neq a_j, 0 \neq k_i \in \mathbf{Z} \right\}.$$

If we identify the element $k_1 a_1 + k_2 a_2 + \cdots + k_l a_l$ with the function $f : S \to \mathbf{Z}$ given by $f(a_i) = k_i$ and $f(a) = 0$ for $a \neq a_i$ for any i, then we can identify $A(S)$ with the set

$$A(S) = \sum_{a \in S} \mathbf{Z} = \left\{ f : S \to \mathbf{Z} \middle| f(a) = 0 \text{ for all but finitely many } a \in S \right\}.$$

Under this identification, we use the operation given by $(f + g)(a) = f(a) + g(a)$.

.

Chapter 3. The Symmetric Group

3.1 Definition: An element $\alpha \in S_n$ can be specified by giving its table of values in the form

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

This is called **array notation** for α.

3.2 Example: In array notation, we have

$$S_3 = \left\{ \begin{pmatrix} 1&2&3\\1&2&3 \end{pmatrix}, \begin{pmatrix} 1&2&3\\1&3&2 \end{pmatrix}, \begin{pmatrix} 1&2&3\\2&1&3 \end{pmatrix}, \begin{pmatrix} 1&2&3\\2&3&1 \end{pmatrix}, \begin{pmatrix} 1&2&3\\3&1&2 \end{pmatrix}, \begin{pmatrix} 1&2&3\\3&2&1 \end{pmatrix} \right\}.$$

Note that S_3 is not abelian because for example

$$\begin{pmatrix} 1&2&3\\2&1&3 \end{pmatrix}\begin{pmatrix} 1&2&3\\3&1&2 \end{pmatrix} = \begin{pmatrix} 1&2&3\\3&2&1 \end{pmatrix} \; , \; \begin{pmatrix} 1&2&3\\3&1&2 \end{pmatrix}\begin{pmatrix} 1&2&3\\2&1&3 \end{pmatrix} = \begin{pmatrix} 1&2&3\\1&3&2 \end{pmatrix}$$

(since the operation is composition, in the product $\alpha\beta$, the permutation β is performed before the permutation α).

3.3 Example: For $n \geq 3$, we can think of D_n as a subgroup of S_n because an element of D_n permutes the elements of $C_n = \left\{ e^{i\,2\pi k/n} \middle| k = 1, 2, \cdots, n \right\}$ and this determines a permutation of $\{1, 2, \cdots, n\}$. For example, in D_6 we have

$$R_1 = \begin{pmatrix} 1&2&3&4&5&6\\2&3&4&5&6&1 \end{pmatrix} \; , \; R_2 = \begin{pmatrix} 1&2&3&4&5&6\\3&4&5&6&1&2 \end{pmatrix}$$
$$F_0 = \begin{pmatrix} 1&2&3&4&5&6\\5&4&3&2&1&6 \end{pmatrix} \; , \; F_1 = \begin{pmatrix} 1&2&3&4&5&6\\6&5&4&3&2&1 \end{pmatrix} .$$

3.4 Definition: When $a_1, a_2, \cdots, a_\ell$ are distinct elements in $\{1, 2, \cdots, n\}$ we write

$$\alpha = (a_1, a_2, \cdots, a_\ell)$$

for the permutation $\alpha \in S_n$ given by

$$\alpha(a_1) = a_2 \; , \; \alpha(a_2) = a_3 \; , \; \cdots \; , \; \alpha(a_{\ell-1}) = a_\ell \; , \; \alpha(a_\ell) = a_1$$
$$\alpha(k) = k \text{ for all } k \notin \{a_1, a_2, \cdots, a_\ell\} .$$

Such a permutation is called a **cycle of length** ℓ or an ℓ**-cycle**.

3.5 Note: We make several remarks.

(1) We have $e = (1) = (2) = \cdots = (n)$.
(2) We have $(a_1, a_2, \cdots, a_\ell) = (a_2, a_3, \cdots, a_\ell, a_1) = (a_3, a_4, \cdots, a_\ell, a_1, a_2) = \cdots$.
(3) An ℓ-cycle with $\ell \geq 2$ can be expressed *uniquely* in the form $\alpha = (a_1, a_2, \cdots, a_\ell)$ with $a_1 = \min\{a_1, a_2, \cdots, a_\ell\}$.
(4) For an ℓ-cycle $\alpha = (a_1, a_2, \cdots, a_\ell)$ we have $|\alpha| = \ell$.
(5) If $n \geq 3$ then we have $(12)(23) = (123)$ and $(23)(12) = (132)$ so S_n is not abelian.

3.6 Definition: Two cycles $\alpha = (a_1, a_2, \cdots, a_\ell)$ and $\beta = (b_1, b_2, \cdots, b_m)$ are said to be **disjoint** when $\{a_1, \cdots, a_\ell\} \cap \{b_1, \cdots, b_m\} = \emptyset$, that is when the a_i and b_j are all distinct. More generally the cycles $\alpha_1 = (a_{1,1}, \cdots, a_{1,\ell_1}), \cdots, \alpha_m = (a_{m,1}, \cdots, a_{m,\ell_m})$ are **disjoint** when all of the $a_{i,j}$ are distinct.

3.7 Note: Disjoint cycles commute. Indeed if $\alpha=(a_1,\cdots,a_\ell)$ and $\beta=(b_1,\cdots,b_m)$ are disjoint, then

$$\begin{aligned}\alpha\big(\beta(a_i)\big)&=\alpha(a_i)=a_{i+1}=\beta(a_{i+1})=\beta\big(\alpha(a_i)\big)\text{ , with subscripts in }\mathbf{Z}_\ell\\ \alpha\big(\beta(b_j)\big)&=\alpha(b_{j+1})=b_{j+1}=\beta(b_j)=\beta\big(\alpha(b_j)\big)\text{ , with subscripts in }\mathbf{Z}_m\\ \alpha\big(\beta(k)\big)&=\alpha(k)=k=\beta(k)=\beta\big(\alpha(k)\big)\text{ for }k\neq a_i,b_j\,.\end{aligned}$$

3.8 Theorem: (*Cycle Notation*) *Every $\alpha\in S_n$ can be written as a product of disjoint cycles. Indeed every $\alpha\neq e$ can be written uniquely in the form*

$$\alpha=(a_{1,1},\cdots,a_{1,\ell_1})(a_{2,1},\cdots,a_{2,\ell_2})\cdots(a_{m,1},\cdots,a_{m,\ell_m})$$

with $m\geq 1$, each $\ell_i\geq 2$, each $a_{i,1}=\min\{a_{i,1},a_{i,2},\cdots,a_{i,\ell_i}\}$ and $a_{1,1}<a_{2,1}<\cdots<a_{m,1}$.

Proof: Let $e\neq\alpha\in S_n$ where $n\geq 2$. To write α in the given form, we must take $a_{1,1}$ to be the smallest element $k\in\{1,2,\cdots,n\}$ with $\alpha(k)\neq k$. Then we must have $a_{1,2}=\alpha(a_{1,1})$, $a_{1,3}=\alpha(a_{1,2})=\alpha^2(a_{1,1})$, and so on. Eventually we must reach ℓ_1 such that $a_{1,1}=\alpha^{\ell_1}(a_{1,1})$, indeed since $\{1,2,\cdots,n\}$ is finite, eventually we find $\alpha^i(a_{1,1})=\alpha^j(a_{1,1})$ for some $1\leq i<j$ and then $a_{1,1}=\alpha^{-i}\alpha^i(a_{1,1})=\alpha^{-i}\alpha^j(a_{1,1})=\alpha^{j-i}(a_{1,1})$. For the smallest such ℓ_1 the elements $a_{1,1},\cdots,a_{1,\ell_1}$ will be disjoint since if we had $a_{1,i}=a_{1,j}$ for some $1\leq i<j\leq\ell_1$ then, as above, we would have $\alpha^{j-i}(a_{11})=a_{11}$ with $1\leq j-i<\ell_1$. This gives us the first cycle $\alpha_1=(a_{1,1},a_{1,2},\cdots,a_{1,\ell_1})$.

If we have $\alpha=\alpha_1$ we are done. Otherwise there must be some $k\in\{1,2,\cdots,n\}$ with $k\notin\{a_{1,1},a_{1,2},\cdots,a_{1,\ell_1}\}$ such that $\alpha(k)\neq k$, and we must choose $a_{2,1}$ to be the smallest such k. As above we obtain the second cycle $\alpha_2=(a_{2,1},a_{2,2},\cdots,a_{2,\ell_2})$. Note that α_2 must be disjoint from α_1 because if we had $\alpha^i(a_{2,1})=\alpha^j(a_{1,1})$ for some i,j then we would have $a_{2,1}=\alpha^{-i}\alpha^i(a_{2,1})=\alpha^{-i}\alpha^j(a_{1,1})=\alpha^{j-i}(a_{1,1})\in\{a_{1,1},\cdots,a_{1,\ell_1}\}$.

At this stage, if $\alpha=\alpha_1\alpha_2$ we are done, and otherwise we continue the procedure.

3.9 Definition: When a permutation $e\neq\alpha\in S_n$ is written in the unique form of the above theorem, we say that α is written in **cycle notation**. We usually write e as $e=(1)$.

3.10 Example: In cycle notation we have

$$\begin{aligned}S_3&=D_3=\big\{(1),(12),(13),(23),(123),(132)\big\}\\ S_4&=\big\{(1),(12),(13),(14),(23),(24),(34),\ (12)(34)\ ,\ (13)(24)\ ,\ (14)(23)\ ,\\ &\qquad(123),(132),(124),(142),(134),(143),(234),(243),\\ &\qquad(1234),(1243),(1324),(1342),(1423),(1432)\big\}\\ D_4&=\big\{I,R_1,R_2,R_3.R_4,R_5,F_0,F_1,F_2,F_3,F_4,F_5\big\}\\ &=\big\{(1),(1234)\ ,\ (13)(24)\ ,\ (1432)\ ,\ (13)\ ,\ (14)(23)\ ,\ (24)\ ,\ (12)(34)\big\}\end{aligned}$$

3.11 Example: For $\alpha=(1352)(46)$, $\beta=(145)(263)\in S_6$, express $\alpha\beta$ in cycle notation.

3.12 Example: Find the number of elements in S_{15} which can be written as a product of 3 disjoint 4-cycles.

Solution: When we write $\alpha=(a_1a_2a_3a_4)(a_5a_6a_7a_8)(a_9a_{10}a_{11}a_{12})$, there are $\binom{15}{12}$ ways to choose the set $\{a_1,\cdots,a_{12}\}$ from $\{1,2,\cdots,15\}$, then there is one choice for a_1 (it must be the smallest of the a_i), then there are 11 choices for a_2, then 10 choices for a_3, then 9 choices for a_4, and then there is only one choice for a_5 (it must be the smallest of the remaining a_i, and so on. Thus there are $\binom{15}{12}\cdot\frac{12!}{12\cdot 8\cdot 4}$ such elements in S_{15}.

3.13 Example: Find the number of elements in S_{20} which can be written as a product of 7 disjoint cycles, with 4 of length 2, 2 of length 3, and 1 of length 4.

Solution: When we write $\alpha = (a_1a_2)(a_3a_4)(a_5a_6)(a_7a_8)\,(b_1b_2b_3)(b_4b_5b_6)\,(c_1c_2c_3c_4)$, there are $\binom{20}{8}$ ways to choose $\{a_1, a_2, \cdots, a_8\}$ from $\{1, 2, \cdots, 20\}$, then $\binom{12}{6}$ ways to choose $\{b_1, \cdots, b_6\}$ from $\{1, \cdots, 20\} \setminus \{a_1, \cdots, a_8\}$, and then there are $\binom{4}{4} = 1$ way to choose $\{c_1, \cdots, c_4)\}$. From the set $\{a_1, \cdots, a_8\}$, there is 1 way to choose a_1, then 7 ways to choose a_2, then 1 way to choose a_3, then 5 ways to choose a_4, then 1 way to choose a_5, then 3 ways to choose a_6, then 1 way to choose a_7 and then 1 way to choose a_8. From the set $\{b_1, \cdots, b_6\}$, there is 1 way to choose b_1, then 5 ways to choose b_2, then 4 ways to choose b_3, then 1 way to choose b_4, then 2 ways to choose b_5 and then 1 way to choose b_6. From the set $\{c_1, \cdots, c_4\}$, there is 1 way to choose c_1, then 3 ways to choose c_2, then 2 ways to choose c_3 and then 1 way to choose c_4. Thus the number of such elements in S_{20} is

$$\binom{20}{8}\binom{12}{6}\binom{4}{4} \cdot \frac{8!}{8\cdot 6\cdot 4\cdot 2} \cdot \frac{6!}{6\cdot 3} \cdot \frac{4!}{4}\,.$$

3.14 Theorem: (*The Order of a Permutation*) *Let $\alpha = \alpha_1\alpha_2\cdots\alpha_m$ where the α_i are disjoint cycles with each α_i of length ℓ_i. Then $|\alpha| = \mathrm{lcm}\{\ell_1, \cdots, \ell_m\}$.*

Proof: Since the α_i are disjoint, if we write $\alpha_k = (a_{k,1}, \cdots, a_{k,\ell_k})$ then we have

$$\alpha(a_{k,1}) = a_{k,2}\ ,\ \alpha^2(a_{k,1}) = a_{k,3}\ ,\ \cdots\ ,\ \alpha^{\ell_m - 1}(a_{k,1}) = a_{k,\ell_m}\ ,\ \alpha^{\ell_m}(a_{k,1}) = a_{k,1}\,.$$

If p is a common multiple of all the ℓ_i, say $p = \ell_i q_i$, then

$$\alpha_i{}^p = \alpha_i{}^{\ell_i q_i} = (\alpha_i{}^{\ell_i})^{q_i} = e^{q_i} = e \text{ for all } i\,.$$

Since the α_i commute, we have $\alpha^p = (\alpha_1\alpha_2\cdots\alpha_m)^p = \alpha_1{}^p\alpha_2{}^p\cdots\alpha_m{}^p = e$.

If, on the other hand, p is not a common multiple of the ℓ_i, then we can choose k so that p is not a multiple of ℓ_k. Write $p = \ell_k q + r$ with $0 < r < \ell_k$. Then

$$\alpha_k{}^p = \alpha_k{}^{\ell_k q + r} = (\alpha_k{}^{\ell_k})^{q_k}\alpha_k{}^r = \alpha_k{}^r$$

and we have $\alpha^p(a_{k,1}) = \alpha_k{}^p(a_{k,1}) = \alpha_k{}^r(a_{k,1}) \neq a_{k,1}$ since $0 < r < \ell_k$, and so $\alpha^p \neq e$.

3.15 Theorem: (*The Conjugacy Class of a Permutation*) *Let $\alpha, \beta \in S_n$. Then α and β are conjugate in S_n if and only if, when written in cycle notation, α and β have the same number of cycles of each length.*

Proof: Write α in cycle notation as $\alpha = (a_{11}, a_{12}, \cdots, a_{1,\ell_1})\cdots(a_{m1}, a_{m2}, \cdots, a_{m,\ell_m})$. Note that for all $\sigma \in S_n$ we have

$$\sigma\alpha\sigma^{-1} = \big(\sigma(a_{11}), \sigma(a_{12}), \cdots, \sigma(a_{1,\ell_1})\big)\cdots\big(\sigma(a_{m1}), \sigma(a_{m2}), \cdots, \sigma(a_{m,\ell_m})\big).$$

Indeed, for the permutation on the right, $\sigma(a_{i,j})$ is sent to $\sigma(a_{i,j+1})$, and on the left, $\sigma(a_{i,j})$ is sent by σ to $a_{i,j}$, which is then sent to $a_{i,j+1}$ by α, which is then sent by σ to $\sigma(a_{i,j+1})$.

3.16 Example: Let $\alpha = (1693)(275)(15873) \in S_{10}$. Find $|\alpha|$.

Solution: First we write α in as a product of *disjoint* cycles. We have $\alpha = (127)(369)(58)$ and so $|\alpha| = \mathrm{lcm}(3, 3, 2) = 6$.

3.17 Example: As an exercise, find the number of elements of each order in S_6.

3.18 Theorem: (*Even and Odd Permutations*) *In S_n, with $n \geq 2$,*
(1) every $\alpha \in S_n$ is a product of 2-cycles,
(2) if $e = (a_1, b_1)(a_2, b_2)\cdots(a_\ell, b_\ell)$ then ℓ is even, that is $\ell = 0$ mod 2, and
(3) if $\alpha = (a_1, b_1)(a_2, b_2)\cdots(a_\ell, b_\ell) = (c_1, d_1)(c_2, d_2)\cdots(c_m, d_m)$ then $\ell = m \mod 2$.

Solution: To prove part (1), note that given $\alpha \in S_n$ we can write α as a product of cycles, and we have

$$(a_1, a_2, \cdots, a_\ell) = (a_1, a_\ell)(a_1, a_{\ell-1})\cdots(a_1, a_2)\,.$$

We shall prove part (2) by induction. First note that we cannot write e as a single 2-cycle, but we can write e as a product of two 2-cycles, for example $e = (1, 2)(1, 2)$. Fix $\ell \geq 3$ and suppose, inductively, that for all $k < \ell$, if we can write e as a product of k 2-cycles the k must be even. Suppose that e can be written as a product of ℓ 2-cycles, say $e = (a_1, b_1)(a_2, b_2)\cdots(a_\ell, b_\ell)$. Let $a = a_1$. Of all the ways we can write e as a product of ℓ 2-cycles, in the form $e = (x_1, y_1)(x_2, y_2)\cdots(x_\ell, y_\ell)$, with $x_i = a$ for some i, choose one way, say $e = (r_1, s_1)(r_2, s_2)\cdots(r_\ell, s_\ell)$ with $r_m = a$ and $r_i, s_i \neq a$ for all $i < m$, with m being as large as possible. Note that $m \neq \ell$ since for $\alpha = (r_1, s_1)\cdots(r_\ell, s_\ell)$ with $r_\ell = a$ and $r_i, s_i \neq a$ for $i < \ell$ we have $\alpha(s_\ell) = a \neq s_\ell$ and so $\alpha \neq e$. Consider the product $(r_m, s_m)(r_{m+1}, s_{m+1})$. This product must be (after possibly interchanging r_{m+1} and s_{m+1}) of one of the forms

$$(a, b)(a, b)\ ,\ (a, b)(a, c)\ ,\ (a, b)(b, c)\ ,\ (a, b)(c, d)$$

where a, b, c, d are distinct. Note that

$$\begin{aligned}(a, b)(a, c) &= (a, c, b) = (b, c)(a, b),\\ (a, b)(b, c) &= (a, b, c) = (b, c)(a, c), \text{ and}\\ (a, b)(c, d) &= (c, d)(a, b)\,,\end{aligned}$$

and so in each of these three cases we could rewrite e as a product of ℓ 2-cycles with the first occurrence of a being farther to the right, contradicting the fact that we chose m to be as large as possible. Thus the product $(r_m, s_m)(r_{m+1}, s_{m+1})$ is of the form $(a, b)(a, b)$. By cancelling these two terms, we can write e as a product of $(\ell - 2)$ 2-cycles. By the induction hypothesis, $(\ell - 2)$ is even, and so ℓ is even.

Finally, to prove part (3), suppose that $\alpha = (a_1, b_1)\cdots(a_\ell, b_\ell) = (c_1, d_1)\cdots(c_m, d_m)$. Then we have

$$e = \alpha\,\alpha^{-1} = (a_1, b_1)\cdots(a_\ell, b_\ell)(c_m, d_m)\cdots(c_1, d_1).$$

By part (2), $\ell + m$ is even, and so $\ell = m \mod 2$.

3.19 Example: Show that

$$S_n = \langle(12), (13), (14), \cdots, (1n)\rangle = \langle(12), (23), (34), \cdots, (n-1, n)\rangle = \langle(12), (123\cdots n)\rangle\,.$$

Solution: By Part (1) of the above theorem, S_n is generated by the set of all 2-cycles (kl). Any 2-cycle (kl) can be written as $(kl) = (1k)(1l)(1k)$ so $S_n = \langle(12), (13), (14), \cdots, (1n)\rangle$. Any 2-cycle of the form $(1k)$ can be written as $(1k) = (12)(23)\cdots(k-1, k)\cdots(23)(12)$ and so $S_n = \langle(12), (23), \cdots, (n-1, n)\rangle$. Any 2-cycle of the form $(k, k+1)$ can be written as $(k, k+1) = (123\cdots n)^{k-1}(12)(123\cdots n)^{-(k-1)}$ and so $S_n = \langle(12)(123\cdots n)\rangle$.

3.20 Definition: For $n \geq 2$, a permutation $\alpha \in S_n$ is called **even** if it can be written as a product of an even number of 2-cycles. Otherwise α can be written as a product of an odd number of 2-cycles, and then it is called **odd**. We define the **parity** of $\alpha \in S_n$ to be

$$(-1)^\alpha = \begin{cases} \ \ 1 \text{ if } \alpha \text{ is even,} \\ -1 \text{ if } \alpha \text{ is odd.} \end{cases}$$

3.21 Theorem: (*Properties of Parity*) *Let $n \geq 2$ and let $\alpha, \beta \in S_n$. Then*
(1) $(-1)^e = 1$,
(2) if α is an ℓ-cycle then $(-1)^\alpha = (-1)^{\ell-1}$,
(3) $(-1)^{\alpha\beta} = (-1)^\alpha(-1)^\beta$, and
(4) $(-1)^{\alpha^{-1}} = (-1)^\alpha$.

Proof: Part (1) holds because, for example, $e = (1,2)(1,2)$. Part (2) holds because we have $(a_1, a_2, \cdots, a_\ell) = (a_1, a_\ell)(a_1, a_{\ell-1}) \cdots (a_1, a_2)$. Part (3) holds because if α is a product of ℓ 2-cycles and β is a product of m 2-cycles then $\alpha\beta$ is a product of $(\ell + m)$ 2-cycles. Part (4) holds because if $\alpha = (a_1, b_1)(a_2, b_2) \cdots (a_\ell, b_\ell)$ then $\alpha^{-1} = (a_\ell, b_\ell) \cdots (a_2, b_2)(a_1, b_1)$.

3.22 Example: Let $\alpha = (1793)(245)(164385) \in S_{10}$. Find $(-1)^\alpha$ and $|\alpha|$.

Solution: By the above theorem, we have $(-1)^\alpha = (-1)^3(-1)^2(-1)^5 = 1$. To find $|\alpha|$, we first write α as a product of *disjoint* cycles. We find that $\alpha = (165793824)$ and so $|\alpha| = 9$.

3.23 Definition: For $n \geq 2$ we define the **alternating group** A_n to be

$$A_n = \left\{\alpha \in S_n \middle| (-1)^\alpha = 1\right\}.$$

Note that $A_n \leq S_n$ by the Properties of Parity Theorem. Note that

$$|A_n| = \tfrac{1}{2}|S_n| = \tfrac{n!}{2}$$

because we have a bijective correspondence

$$F : \left\{\alpha \in S_n \middle| (-1)^\alpha = 1\right\} \to \left\{\alpha \in S_n \middle| (-1)^\alpha = -1\right\}$$

given by $F(\alpha) = (12)\alpha$.

3.24 Remark: The rotation group of the regular tetrahedron can be identified with A_4 by labelling the vertices of the tetrahedron by 1, 2, 3 and 4 and identifying each rotation with a permutation of $\{1, 2, 3, 4\}$.

3.25 Example: Show that A_n is generated by the set of all 3-cycles, then show that for any $a \neq b \in \{1, 2, \cdots, n\}$, A_n is generated by the 3-cycles of the form (abk) with $k \neq a, b$.

Solution: We already know that every permutation in A_n is equal to a product of an even number of 2-cycles. Every product of a pair of 2-cycles is of one of the forms $(ab)(ab)$, $(ab)(ac)$ or $(ab)(cd)$, where a, b, c, d are distinct, and we have

$$(ab)(ab) = (abc)(acb)\ ,\ (ab)(ac) = (acb)\ ,\ (ab)(cd) = (adc)(abc)\,,$$

and so A_n is generated by the set of all 3-cycles. Now fix $a, b \in \{1, 2, \cdots, n\}$ with $a \neq b$. Note that every 3-cycle is of one of the forms (abk), (akb), (akl), (bkl) or (klm), where a, b, k, l, m are all distinct, and we have

$$(akb) = (abk)^2\ ,\ (akl) = (abl)(abk)^2\ ,\ (bkl) = (abl)^2(abk)\ ,\ (klm) = (abk)^2(abm)(abl)^2(abk)\,.$$

.

Chapter 4. Homomorphisms and Isomorphisms of Groups

4.1 Note: We recall the following terminology. Let X and Y be sets. When we say that f is a **function** or a **map** from X to Y, written $f : X \to Y$, we mean that for every $x \in X$ there exists a unique corresponding element $y = f(x) \in Y$. The set X is called the **domain** of f and the **range** or **image** of f is the set $\text{Image}(f) = f(X) = \{f(x)\big|x \in X\}$. For a set $A \subseteq X$, the **image** of A under f is the set $f(A) = \{f(a)\big|a \in A\}$ and for a set $B \subseteq Y$, the **inverse image** of B under f is the set $f^{-1}(B) = \{x \in X\big|f(x) \in B\}$.

For a function $f : X \to Y$, we say f is **one-to-one** (written $1:1$) or **injective** when for every $y \in Y$ there exists at most one $x \in X$ such that $y = f(x)$, we say f is **onto** or **surjective** when for every $y \in Y$ there exists at least one $x \in X$ such that $y = f(x)$, and we say f is **invertible** or **bijective** when f is 1:1 and onto, that is for every $y \in Y$ there exists a unique $x \in X$ such that $y = f(x)$. When f is invertible, the **inverse** of f is the function $f^{-1} : Y \to X$ defined by $f^{-1}(y) = x \iff y = f(x)$.

For $f : X \to Y$ and $g : Y \to Z$, the **composite** $g \circ f : X \to Z$ is given by $(g \circ f)(x) = g(f(x))$. Note that it f and g are both injective then so is the composite $g \circ f$, and if f and g are both surjective then so is $g \circ f$.

4.2 Definition: Let G and H be groups. A group **homomorphism** from G to H is a function $\phi : G \to H$ such that

$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in G$, or to be more precise, such that $\phi(a * b) = \phi(a) \times \phi(b)$ for all $a, b \in G$, where $*$ is the operation on G and $\times$ is the operation on H. The **kernel** of ϕ is the set

$$\text{Ker}(\phi) = \phi^{-1}(e) = \{a \in G\big|\phi(a) = e\}$$

where $e = e_H$ is the identity in H, and the **image** (or **range**) of ϕ is

$$\text{Image}(\phi) = \phi(G) = \{\phi(a)\big|a \in G\}\,.$$

A group **isomorphism** from G to H is a bijective group homomorphism $\phi : G \to H$. For two groups G and H, we say that G and H are **isomorphic** and we write $G \cong H$ when there exists an isomorphism $\phi : G \to H$. An **endomorphism** of a group G is a homomorphism from G to itself. An **automorphism** of a group G is an isomorphism from G to itself. The set of all homomorphisms from G to H, the set of all isomorphisms from G to H, the set of all endomorphisms of G, and the set of all automorphisms of G will be denoted by

$$\text{Hom}(G, H)\ ,\ \text{Iso}(G, H)\ ,\ \text{End}(G)\ ,\ \text{Aut}(G)\,.$$

4.3 Remark: In algebra, we consider isomorphic groups to be (essentially) equivalent. The **classification problem** for finite groups is to determine, given any $n \in \mathbf{Z}^+$, the complete list of all groups, up to isomorphism, of order n.

4.4 Example: The groups U_{12} and ${\mathbf{Z}_2}^2$ are isomorphic. One way to see this is to compare their operation tables.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

We see that all the entries in these tables correspond under the map $\phi : U_{12} \to {\mathbf{Z}_2}^2$ given by $\phi(1) = (0,0)$, $\phi(5) = (0,1)$, $\phi(7) = (1,0)$ and $\phi(1,1) = (1,1)$, so ϕ is an isomorphism.

4.5 Example: Let G be a group and let $a \in G$. Then the map $\phi_a : \mathbf{Z} \to G$ given by $\phi_a(k) = a^k$ is a group homomorphism since $\phi_a(k+\ell) = a^{k+\ell} = a^k a^\ell = \phi_a(k)\phi_a(\ell)$. The image of ϕ_a is

$$\text{Image}(\phi_a) = \left\{a^k \middle| k \in \mathbf{Z}\right\} = \langle a \rangle$$

and the kernel of ϕ_a is

$$\text{Ker}(\phi_a) = \left\{k \in \mathbf{Z} \middle| a^k = e\right\} = \begin{cases} \langle n \rangle = n\mathbf{Z} \text{ , if } |a| = n, \\ \langle 0 \rangle = \{0\} \text{ , if } |a| = \infty. \end{cases}$$

4.6 Example: Let G be a group and let $a \in G$. If $|a| = \infty$ then the map $\phi_a : \mathbf{Z} \to \langle a \rangle$ given by $\phi(k) = a^k$ is an isomorphism, and if $|a| = n$ then the map $\phi_a : \mathbf{Z}_n \to \langle a \rangle$ given by $\phi_a(k) = a^k$ is an isomorphism (note that ϕ_a is well-defined because if $k = \ell \bmod n$ then $a^k = a^\ell$ by Theorem 2.3). In each case, ϕ is a homomorphism since $a^{k+\ell} = a^k a^\ell$ and ϕ is bijective by Theorem 2.3.

4.7 Example: When R is a commutative ring with 1, the map $\phi : GL_n(R) \to R^*$ given by $\phi(A) = \det(A)$ is a group homomorphism since $\det(AB) = \det(A)\det(B)$. The kernel is

$$\text{Ker}(\phi) = \left\{A \in GL_n(R) \middle| \det(A) = 1\right\} = SL_n(R)$$

and the image is

$$\text{Image}(\phi) = \left\{\det(A) \middle| A \in GL_n(R)\right\} = R^*$$

since for $a \in R^*$ we have $\det\big(\text{diag}(a, 1, 1, \cdots, 1)\big) = a$.

4.8 Example: The map $\phi : \mathbf{R} \to \mathbf{R}^+$ given by $\phi(x) = e^x$ is a group isomorphism since it is bijective and $\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$.

4.9 Example: The map $\phi : SO_2(\mathbf{R}) \to \mathbf{S}^1$ given by $\phi(R_\theta) = e^{i\,\theta}$ is a group isomorphism.

4.10 Theorem: *Let G and H be groups and let $\phi : G \to H$ be a group homomorphism. Then*

(1) $\phi(e_{\text{G}}) = e_{\text{H}}$,
(2) $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$,
(3) $\phi(a^k) = \phi(a)^k$ for all $a \in G$ and all $k \in \mathbf{Z}$, and
(4) for $a \in G$, if $|a|$ is finite then $|\phi(a)|$ divides $|a|$.

Proof: To prove (1), note that $\phi(e_{\text{G}}) = \phi(e_{\text{G}}\, e_{\text{G}}) = \phi(e_{\text{G}})\phi(e_{\text{G}})$ so $\phi(e_{\text{G}}) = e_{\text{H}}$ by cancellation. To prove (2) note that $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_{\text{G}}) = e_{\text{H}}$, so $\phi(a)^{-1} = \phi(a^{-1})$ by cancellation. For part (3), note first that $\phi(a^0) = \phi(a)^0$ by part (1), and then note that when $k \in \mathbf{Z}^+$ we have $\phi(a^k) = \phi(aa\cdots a) = \phi(a)\phi(a)\cdots\phi(a) = \phi(a)^k$ and hence also $\phi(a^{-k}) = \phi\big((a^{-1})^k\big) = \phi(a^{-1})^k = \big(\phi(a)^{-1}\big)^k = \phi(a)^{-k}$. For part (4) note that if $|a| = n$ then we have $\phi(a)^n = \phi(a^n) = \phi(e_{\text{G}}) = e_{\text{H}}$ and so $|\phi(a)|$ divides n by Theorem 2.3.

4.11 Theorem: *Let G, H and K be groups. Let $\phi : G \to H$ and $\psi : H \to K$ be group homomorphisms. Then*

(1) the identity $I : G \to G$ given by $I(x) = x$ for all $x \in G$, is an isomorphism,
(2) the composite $\psi \circ \phi : G \to K$ is a group homomorphism, and
(3) if $\phi : G \to H$ is an isomorphism then so is its inverse $\phi^{-1} : H \to G$.

Proof: We prove part (3) and leave the proofs of (1) and (2) as an exercise. Suppose that $\phi : G \to H$ is an isomorphism. Let $\psi = \phi^{-1} : H \to G$. We know that ψ is bijective, so we just need to show that ψ is a homomorphism. Let $c, d \in H$. Let $a = \phi(c)$ and $b = \psi(d)$. Since ϕ is a homomorphism we have $\phi(ab) = \phi(a)\phi(b)$, and so

$$\psi(cd) = \psi\big(\phi(a)\phi(b)\big) = \psi\big(\phi(ab)\big) = ab = \psi(c)\psi(d)\,.$$

4.12 Corollary: *Isomorphism is an equivalence relation on the class of groups. This means that for all groups G, H and K we have*

(1) $G \cong G$,
(2) if $G \cong H$ and $H \cong K$ then $G \cong K$, and
(3) if $G \cong H$ then $H \cong G$.

4.13 Corollary: *For a group G, $\text{Aut}(G)$ is a group under composition.*

4.14 Theorem: *Let $\phi : G \to H$ be a homomorphism of groups. Then*

(1) if $K \leq G$ then $\phi(K) \leq H$, in particular $\text{Image}(\phi) \leq H$,
(2) if $L \leq H$ then $\phi^{-1}(L) \leq G$, in particular $\text{Ker}(\phi) \leq G$.

Proof: The proof is left as an exercise.

4.15 Theorem: *Let $\phi : G \to H$ be a homomorphism of groups. Then*

(1) ϕ is injective if and only if $\text{Ker}(\phi) = \{e\}$, and
(2) ϕ is surjective if and only if $\text{Image}(\phi) = H$.

Proof: The proof is left as an exercise.

4.16 Theorem: *Let $\phi : G \to H$ be an isomorphism of groups. Then*
(1) G is abelian if and only if H is abelian,
(2) for $a \in G$ we have $\big|\phi(a)\big| = |a|$,
(3) G is cyclic with $G = \langle a \rangle$ if and only if H is cyclic with $H = \langle \phi(a) \rangle$,
(4) for $n \in \mathbf{Z}^+$ we have $\Big|\big\{a \in G \big| |a| = n\big\}\Big| = \Big|\big\{b \in H \big| |b| = n\big\}\Big|$,
(5) for $K \leq G$ the restriction $\phi : K \to \phi(K)$ is an isomorphism of groups, and
(6) for any group C we have $\Big|\big\{K \leq G \big| K \cong C\big\}\Big| = \Big|\big\{L \leq H \big| L \cong C\big\}\Big|$.

Proof: The proof is left as an exercise.

4.17 Example: Note that $\mathbf{Q}^* \not\cong \mathbf{R}^*$ since $|\mathbf{Q}^*| \neq |\mathbf{R}^*|$. Similarly, $GL_3(\mathbf{Z}_2) \not\cong S_5$ because $\big|GL_3(\mathbf{Z}_2)\big| = 168$ but $|S_5| = 120$.

4.18 Example: $\mathbf{C}^* \not\cong GL_2(\mathbf{R})$ since $\mathbf{C}^*$ is abelian but $GL_n(\mathbf{R})$ is not. Similarly, $S_4 \not\cong U_{35}$ because U_{35} is abelian but S_4 is not.

4.19 Example: $\mathbf{R}^* \not\cong \mathbf{C}^*$ since $\mathbf{C}^*$ has elements of order $n \geq 3$, for example $|i| = 4$ in $\mathbf{C}^*$, but $\mathbf{R}^*$ has no elements of order $n \geq 3$, indeed in $\mathbf{R}^*$, $|1| = 1$ and $|-1| = 2$ and for $x \neq \pm 1$ we have $|x| = \infty$.

4.20 Example: Determine whether $U_{35} \cong \mathbf{Z}_{24}$.

Solution: In U_{35} we have

k	0	1	2	3	4	5	6	7	8	9	10	11	12
2^k	1	2	4	8	16	32	29	23	11	22	9	18	1

We notice that U_{35} has at least two elements of order 2, namely 29 and 34, but $\mathbf{Z}_{24}$ has only one element of order 2, namely 12. Thus $U_{35} \not\cong \mathbf{Z}_{24}$.

4.21 Theorem: *Let $a, b \in \mathbf{Z}^+$ with $\gcd(a, b) = 1$. Then*
(1) $\mathbf{Z}_{ab} \cong \mathbf{Z}_a \times \mathbf{Z}_b$ and
(2) $U_{ab} \cong U_a \times U_b$.

Proof: We prove part (2) (the proof of part (1) is similar). Define $\phi : U_{ab} \to U_a \times U_b$ by $\phi(k) = (k, k)$. This map ϕ is well-defined because if $k = \ell$ mod ab then $k = \ell$ mod a and $k = \ell$ mod b and because if $\gcd(k, ab) = 1$ so that $k \in U_{ab}$ then $\gcd(k, a) = \gcd(k, b) = 1$. Also, ϕ is a group homomorphism since $\phi(k\ell) = (k\ell, k\ell) = (k, k)(\ell, \ell) = \phi(k)\phi(\ell)$. Finally note that ϕ is bijective by the Chinese Remainder Theorem, indeed ϕ is onto because given $k \in U_a$ and $\ell \in U_b$ there exists $x \in \mathbf{Z}$ with $x = k$ mod a and $x = \ell$ mod b and we then have $\gcd(x, a) = \gcd(k, a) = 1$ and $\gcd(x, b) = \gcd(\ell, b) = 1$ so that $\gcd(x, ab) = 1$, that is $x \in U_{ab}$, and ϕ is 1:1 because this solution x is unique modulo ab.

4.22 Corollary: *If $n = \prod_{i=1}^{\ell} {p_i}^{k_i}$ where the p_i are distinct primes and each $k_i \in \mathbf{Z}^+$ then*

$$\phi(n) = \prod_{i=1}^{\ell} \left({p_i}^{k_i} - {p_i}^{k_i - 1}\right) = n \cdot \prod_{i=1}^{\ell} \left(1 - \tfrac{1}{p_i}\right).$$

4.23 Definition: Let G be a group. For $a \in G$, we define **left multiplication** by a to be the map $L_a : G \to G$ given by

$$L_a(x) = ax \text{ for } x \in G\,.$$

Note that $L_e = I$ (since $L_e(x) = ex = x = I(x)$ for all $x \in G$) and $L_a L_b = L_{ab}$ since $L_a\big(L_b(x)\big) = L_a(bx) = abx = L_{ab}(x)$ for all $x \in G$. Similarly, we define **right-multiplication** by a to be the map $R_a : G \to G$ given by $R_a(x) = ax$ for $x \in G$. Also, we define **conjugation** by a to be the map $C_a : G \to G$ by

$$C_a(x) = a\,x\,a^{-1} \text{ for } x \in G\,.$$

The map $L_a : G \to G$ is not necessarily a group homomorphism since $L_a(xy) = axy$ while $L_a(x)L_a(y) = axay$. On the other hand, the map $C_a : G \to G$ is a group homomorphism because $C_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = C_a(x)C_a(y)$. Indeed C_a is an automorphism of G because it is invertible with ${C_a}^{-1} = C_{a^{-1}}$. An automorphism of G of the form C_a is called an **inner automorphism** of G. The set of all inner automorphisms of G is denoted by $\text{Inn}(G)$, so we have

$$\text{Inn}(G) = \big\{C_a \big| a \in G\big\}\,.$$

Note that $\text{Inn}(G) \leq \text{Aut}(G)$ because $I = C_e$, $C_a C_b = C_{ab}$ and ${C_a}^{-1} = C_{a^{-1}}$. Note that when $H \leq G$, the restriction of the conjugation map C_a gives an isomorphism from H to the group

$$C_a(H) = aHa^{-1} = \big\{aha^{-1}\big|h \in H\big\} \cong H\,.$$

The isomorphic groups H and $C_a(H) = aHa^{-1}$ are called **conjugate** subgroups of G.

4.24 Example: As an exercise, find $\text{Inn}(D_4)$ and show that $\text{Inn}(D_4) \neq \text{Aut}(D_4)$.

4.25 Example: Let G be a finite set with $|G| = n$. Let $S = \{1, 2, \cdots, n\}$ and let $f : G \to S$ be a bijection. The map $C_f : \text{Perm}(G) \to S_n$ given by $C_f(g) = f\,g\,f^{-1}$ is a group isomorphism. Indeed, C_f is well-defined since when $g \in \text{Perm}(G)$ the map $f\,g\,f^{-1}$ is invertible with $(f\,g\,f^{-1})^{-1} = f\,g^{-1}f^{-1}$, and C_f is a group homomorphism since $C_f(gh) = fghf^{-1} = fgf^{-1}fhf^{-1} = C_f(g)C_f(h)$, and C_f is bijective with inverse ${C_f}^{-1} = C_{f^{-1}}$.

4.26 Theorem: (*Cayley's Theorem*) *Let G be a group.*

(1) G is isomorphic to a subgroup of $\text{Perm}(G)$.
(2) If $|G| = n$ then G is isomorphic to a subgroup of S_n.

Proof: Define $\phi : G \to \text{Perm}(G)$ by $\phi(a) = L_a$. Note that $L_a \in \text{Perm}(G)$ because L_a is invertible with inverse ${L_a}^{-1} = L_{a^{-1}}$. Also, ϕ is a group homomorphism because $\phi(ab) = L_{ab} = L_a L_b$ and ϕ is injective because $L_a = I \Longrightarrow a = e$ (indeed if $L_a = I$ then $a = ae = L_a(e) = I(e) = e$). Thus ϕ is an isomorphism from G to $\phi(G)$, which is a subgroup of $\text{Perm}(G)$.

Now suppose that $|G| = n$, say $f : G \to \{1, 2, \cdots, n\}$ is a bijection. Then the map $C_f \circ \phi$ is an injective group homomorphism (where $C_f(g) = fgf^{-1}$, as above), and so G is isomorphic to $C_f\big(\phi(G)\big)$ which is a subgroup of S_n.

4.27 Example: Show that $\mathrm{Hom}(\mathbf{Z},G)=\big\{\phi_a\big|a\in G\big\}$, where $\phi_a(k)=a^k$.

Solution: Let $\phi\in\mathrm{Hom}(\mathbf{Z},G)$. Let $a=\phi(1)$. Then for all $k\in\mathbf{Z}$ we have $\phi(k)=\phi(k\cdot 1)=\phi(1)^k=a^k$, and so $\phi=\phi_a$. On the other hand, note that for $a\in G$ the map ϕ_a given by $\phi_a(k)=a^k$ is a group homomorphism because $\phi_a(k+l)=a^{k+l}=a^ka^l=\phi_a(k)\phi_a(l)$.

4.28 Example: Show that $\mathrm{Hom}(\mathbf{Z}_n,G)=\big\{\phi_a\big|a\in G,a^n=e\big\}$, where $\phi_a(k)=a^k$.

Solution: Let $\phi\in\mathrm{Hom}(\mathbf{Z}_n,G)$. Let $a=\phi(1)$. Then for all $k\in\mathbf{Z}$ we have $\phi(k)=\phi(k\cdot 1)=\phi(1)^k=a^k$ so that $\phi=\phi_a$, and we have $a^n=\phi(n)=\phi(0)=e$. On the other hand, note that for $a\in G$ with $a^n=e$, the map ϕ_a is well-defined because if $k=l \bmod n$ the $a^k=a^l$ and it is a homomorphism because $a^{k+l}=a^ka^l$.

4.29 Example: As an exercise, describe $\mathrm{Hom}\big(\mathbf{Z}_n\times\mathbf{Z}_m,G\big)$.

4.30 Example: As an exercise, describe $\mathrm{Hom}(D_n,G)$.

.

Chapter 5. Cosets, Normal Subgroups, and Quotient Groups

5.1 Definition: Let G be a group with operation $*$, let $H \leq G$ and let $a \in G$. The **left coset** of H in G containing a is the set

$$a * H = \{ax \big| x \in H\}.$$

Similarly the **right coset** of H in G containing a is the set $H * a = \{xa \big| x \in H\}$. Usually, unless the operation is addition, we write $a * H$ as aH and we write $H * a$ as Ha. We denote the set of left cosets of H in G by G/H so we have

$$G/H = \{aH \big| a \in G\}.$$

The **index** of H in G, denoted by $[G : H]$ is the cardinality of the set of cosets, that is

$$[G : H] = \big|G/H\big|.$$

When G is abelian there is no difference between left and right cosets so we simply call them **cosets**.

5.2 Example: In the group $\mathbf{Z}_{12}$, the cosets of $H = \langle 4 \rangle = \{0, 4, 8\}$ are

$$\begin{aligned} 0 + H = 4 + H = 8 + H &= \{0, 4, 8\} = H \\ 1 + H = 5 + H = 9 + H &= \{1, 5, 9\} \\ 2 + H = 6 + H = 10 + H &= \{2, 6, 10\} \\ 3 + H = 7 + H = 11 + H &= \{3, 7, 11\} \end{aligned}$$

5.3 Example: In the group $\mathbf{Z}$, for $n \in \mathbf{Z}^+$, the cosets of $\langle n \rangle = n\mathbf{Z}$ are

$$k + n\mathbf{Z} = \{\cdots, k - 2n, k - n, k, k + n, k + 2n, \cdots\} \text{ where } k \in \mathbf{Z}.$$

These are exactly the elements of $\mathbf{Z}_n$, so we have $\mathbf{Z}/\langle n \rangle = \mathbf{Z}_n$.

5.4 Theorem: *Let G be a group, let $H \leq G$, and let $a, b \in G$. Then*
(1) $b \in aH \iff a^{-1}b \in H \iff aH = bH$,
(2) either $aH = bH$ or $aH \cap bH = \emptyset$, and
(3) $|aH| = |H|$.
Analogous results hold for right cosets.

Proof: If $b \in aH$, say $b = ah$ with $h \in H$, then $a^{-1}b = h \in H$. Conversely if $a^{-1}b \in H$ then $b = ah \in aH$. Thus we have $b \in aH \iff a^{-1}b \in H$. Now suppose that $b \in aH$, say $b = ah$ with $h \in H$. Let $x \in aH$, say $x = ak$ with $k \in H$. Then $x = ak = bh^{-1}k \in bH$. Thus $aH \subseteq bH$. Let $y \in bH$, say $y = bl$ with $l \in H$. Then $y = bl = ahl \in aH$. Thus $bH \subseteq aH$. Conversely, suppose that $aH = bH$. Then $b = be \in bH = aH$. This completes the proof of (1).

To prove (2), suppose that $aH \cap bH \neq \emptyset$. Choose $x \in aH \cap bH$, say $x = ah = bl$ with $h, l \in H$. Then $a^{-1}b = hl^{-1} \in H$ so $aH = bH$ by (1).

To prove (3), define $\phi : H \to aH$ by $\phi(h) = ah$. Then ϕ is clearly surjective, and ϕ is injective since if $\phi(h) = \phi(k)$ then $ah = ak$ and so $h = k$ by cancellation.

5.5 Corollary: (*Lagrange's Theorem*) *Let G be a group and let $H \le G$. Then*

$$|G| = |G/H|\,|H|\,.$$

Proof: The above theorem shows that the group G is partitioned into left cosets and that these cosets all have the same cardinality.

5.6 Corollary: *Let G be a finite group, let $H \le G$ and let $a \in G$. Then $|H|$ divides $|G|$ and $|a|$ divides $|G|$.*

5.7 Corollary: (*The Euler-Fermat Theorem*) *For $a \in U_n$ we have $a^{\phi(n)} = 1$.*

5.8 Corollary: (*The Classification of Groups of Order p*) *Let p be prime. Let G be a group with $|G| = p$. Then $G \cong \mathbf{Z}_p$.*

Proof: Let $a \in \mathbf{Z}_p$ with $a \neq e$. Since $|a|$ divides $|G| = p$ we have $|a| = 1$ or $|a| = p$. Since $a \neq e$, $|a| \neq 1$ so $|a| = p$. Since $\langle a \rangle = |a| = p = |G|$ and $\langle a \rangle \subseteq G$ we have $\langle a \rangle = G$ and so $G = \langle a \rangle \cong \mathbf{Z}_p$.

5.9 Theorem: *Let G be a group and let $H \le G$. The following are equivalent.*
(1) we can define a binary operation $*$ on G/H by $(aH) * (bH) = (ab)H$,
(2) $aha^{-1} \in H$ for all $a \in G$, $h \in H$, and
(3) $aH = Ha$ for all $a \in G$.
(4) $aHa^{-1} = H$ for all $a \in G$.
In this case, G/H is a group under the above operation $*$ with identity $eH = H$.

Proof: Suppose that we can define an operation $*$ on G/H by $(aH) * (bH) = (ab)H$. The fact that this operation is well-defined means that for all $a_1, a_2, b_1, b_2 \in G$, if $a_1H = a_2H$ and $b_1H = b_2H$ then $(a_1b_1)H = (a_2b_2)H$, or equivalently if $a_1^{-1}a_2 \in H$ and ${b_1}^{-1}b_2 \in H$ then $(a_1b_1)^{-1}(a_2b_2) \in H$, that is ${b_1}^{-1}{a_1}^{-1}a_2b_2 \in H$. For ${a_1}^{-1}a_2 = h \in H$ and ${b_1}^{-1}b_2 = k \in H$, we have ${b_1}^{-1}{a_1}^{-1}a_2b_2 = {b_1}^{-1}h\,b_2 = {b_1}^{-1}b_2{b_2}^{-1}k\,b_2 = k{b_2}^{-1}h\,b_2$, and this lies in H if and only if ${b_2}^{-1}h\,b_2 \in H$. This proves that (1) $\iff$ (2).

Suppose that (2) holds and let $a \in G$. Let $x \in aH$, say $x = ah$ with $h \in H$. Then $x = ah = aha^{-1}a \in Ha$ since $aha^{-1} \in H$. Thus $aH \subseteq Ha$. Now let $y \in Ha$, say $y = ka$ with $k \in H$. Then $y = ka = aa^{-1}ka \in aH$ since $a^{-1}ka \in H$ by (2). Thus $Ha \subseteq Ha$. This proves that (2) $\Longrightarrow$ (3).

Conversely, suppose that (3) holds. Let $a \in G$ and $h \in H$. Then $ah \in aH = Ha$ so we can choose $k \in H$ so that $ah = ka$. Then we have $aha^{-1} = kaa^{-1} = k \in H$. This proves that (3) $\Longrightarrow$ (2).

The proof that (3) $\iff$ (4) is left as an exercise.

Now suppose that (1) holds and let $*$ be the above operation. We claim that G/H is a group. Indeed, the operation $*$ is associative since

$$\big((aH)*(bH)\big)*(cH) = \big((ab)H\big)*(cH) = (abc)H = (aH)*\big((bc)H\big) = (aH)*\big((bH)*(cH)\big)\,,$$

the coset $eH = H$ is the identity for G/H since for $a \in G$ we have

$$(aH) * (eH) = (ae)H = aH \;\text{ and }\; (eH) * (aH) = (ea)H = aH\,,$$

and for $a \in G$, the inverse of the coset aH is the coset $a^{-1}H$ since

$$(aH) * (a^{-1}H) = (a\,a^{-1})H = eH \;\text{ and }\; (a^{-1}H) * (aH) = (a^{-1}a)H = eH\,.$$

5.10 Definition: Let G be a group and let $H \leq G$. If H satisfies the equivalent conditions of the above theorem, then we say that H is a **normal** subgroup of G and we write $H \trianglelefteq G$. When $H \trianglelefteq G$, the group G/H is called the **quotient group** of G by H.

5.11 Theorem: (*The First Isomorphism Theorem*)
(1) if $\phi : G \to H$ is a group homomorphism and $K = \mathrm{Ker}(\phi)$ then $K \trianglelefteq G$ and $G/K \cong \phi(G)$, indeed the map $\Phi : G/K \to \phi(G)$ given by $\Phi(aK) = \phi(a)$ is a group isomorphism.
(2) if $K \trianglelefteq G$ then the map $\phi : G \to G/K$ given by $\phi(a) = aK$ is a group homomorphism with $\mathrm{Ker}(\phi) = K$.

Proof: To prove (1), let $\phi : G \to H$ be a group homomorphism and let $K = \mathrm{Ker}(\phi)$. Let $a \in G$ let $k \in K$ so $\phi(k) = e$. Then $\phi(aka^{-1}) = \phi(a)\phi(k)\phi(a^{-1}) = \phi(a)\phi(a)^{-1} = e$ and so $aka^{-1} \in \mathrm{Ker}(\phi) = K$. This shows that $K \trianglelefteq G$. Define $\Phi : G/H \to \phi(G)$ by $\Phi(aK) = \phi(a)$. Note that Φ is well-defined since if $aK = bK$ then $a^{-1}b \in K$ so we have $\phi(a)^{-1}\phi(b) = \phi(a^{-1}b) = e$ and hence $\phi(a) = \phi(b)$. Note that Φ is a group homomorphism since $\Phi\big((aK)(bK)\big) = \Phi\big((ab)K\big) = \phi(ab)\phi(a)\phi(b) = \Phi(aK)\Phi(bK)$. Finally note that Φ is clearly onto, and Φ is 1:1 since if $\Phi(aK) = e$ then $\phi(a) = e$ so $a \in K$ and hence $aK = K$, which is the identity element of G/K.

To prove (2) let $K \trianglelefteq G$. Define $\phi : G \to G/K$ by $\phi(a) = aK$. Then ϕ is a group homomorphism since $\phi(ab) = (ab)K = (aK)(bK) = \phi(a)\phi(b)$, and $\mathrm{Ker}(\phi) = K$ since for $a \in G$ we have $a \in \mathrm{Ker}(\phi) \iff \phi(a) = eK \iff aK = eK \iff a \in eK = K$.

5.12 Theorem: (*The Second Isomorphism Theorem*) *Let G be a group, let $H \leq G$ and let $K \trianglelefteq G$. Then $K \cap H \trianglelefteq H$, $KH = \langle K \cup H \rangle$, and $H\big/(K \cap H) \cong KH\big/K$.*

Proof: The proof is left as an exercise.

5.13 Theorem: (*The Third Isomorphism Theorem*) *Let G be a group and let $H, K \trianglelefteq G$ with $K \leq H$. Then $H/K \trianglelefteq G/K$ and $(G/K)\big/(H/K) \cong G/H$.*

Proof: The proof is left as an exercise.

5.14 Example: The map $\phi : \mathbf{Z} \to \mathbf{Z}_n$ given by $\phi(k) = k$ is a group homomorphism with $\mathrm{Image}(\phi) = \langle n \rangle$ and $\mathrm{Ker}(\phi) = \langle n \rangle$, so we have $\mathbf{Z}\big/\langle n \rangle \cong \mathbf{Z}_n$ (in fact $\mathbf{Z}\big/\langle n \rangle = \mathbf{Z}_n$).

5.15 Example: The map $\phi : \mathbf{R} \to \mathbf{S}^1$ given by $\phi(t) = e^{i\,2\pi t}$ is a group homomorphism, since $e^{i\,2\pi(s+t)} = e^{i\,2\pi s}e^{i\,2\pi t}$, with $\mathrm{Image}(\phi) = \mathbf{S}^1$ and $\mathrm{Ker}(\phi) = \mathbf{Z}$ so we have $\mathbf{R}\big/\mathbf{Z} \cong \mathbf{S}^1$.

5.16 Example: The map $\phi : \mathbf{C}^* \to \mathbf{R}^+$ given by $\phi(z) = ||z||$ is a group homomoprphism, since $||zw|| = ||z||\,||w||$, with $\mathrm{Image}(\phi) = \mathbf{R}^+$ and $\mathrm{Ker}(\phi) = \mathbf{S}^1$ so we have $\mathbf{C}^*\big/\mathbf{S}^1 \cong \mathbf{R}^+$.

5.17 Example: The map $\phi : \mathbf{C}^* \to \mathbf{S}^1$ given by $\phi(z) = \frac{z}{||z||}$, is a group homomorphism, since $\frac{zw}{||zw||} = \frac{z}{||z||}\,\frac{w}{||w||}$, with $\mathrm{Image}(\phi) = \mathbf{S}^1$ and $\mathrm{Ker}(\phi) = \mathbf{R}^+$ and so $\mathbf{C}^*\big/\mathbf{R}^+ \cong \mathbf{S}^1$.

5.18 Example: When R is a commutative ring with 1, the map $\phi : GL_n(R) \to R^*$ given by $\phi(A) = \det(A)$ is a group homomorphism, since $\det(AB) = \det(A)\det(B)$, and it is surjective since for $a \in R^*$ we have $A = \mathrm{diag}(a, 1, \cdots, 1) \in GL_n(R)$ and $\det(A) = a$, and we have $\mathrm{Ker}(\phi) = \big\{A \in GL_n(R)\big|\det(A) = 1\big\} = SL_n(R)$, and so $SL_n(R) \trianglelefteq GL_n(R)$ with $GL_n(R)\big/SL_n(R) \cong R^*$.

5.19 Example: For $n \geq 2$, the map $\phi : S_n \to \mathbf{Z}^* = \{\pm 1\}$ given by $\phi(\alpha) = (-1)^\alpha$ is a group homomorphism since $(-1)^{\alpha\beta} = (-1)^\alpha(-1)^\beta$, and it is surjective since $(-1)^e = 1$ and $(-1)^{(12)} = -1$, and we have $\mathrm{Ker}(\phi) = \big\{\alpha \in S_n\big|(-1)^\alpha = 1\big\} = A_n$, and so $A_n \trianglelefteq S_n$ with $S_n\big/A_n \cong \mathbf{Z}^* = \{\pm 1\}$.

5.20 Example: Let $H = \big\langle (6,2),(3,6)\big\rangle \leq \mathbf{Z}^2$. As an exercise, show that $\big|\mathbf{Z}^2/H\big| = 30$ and that $\mathbf{Z}^2/H$ is cyclic, then find a surjective group homomorphism $\phi : \mathbf{Z}^2 \to \mathbf{Z}_{30}$ with $\mathrm{Ker}(\phi) = H$.

5.21 Example: The map $\phi : G \to \mathrm{Aut}(G)$ given by $\phi(a) = C_a$ (where C_a is conjugation by a, given by $C_a(x) = axa^{-1}$) is a group homomorphism since $C_{ab} = C_a C_b$, and we have $\mathrm{Image}(\phi) = \big\{C_a \big| a \in G\big\} = \mathrm{Inn}(G)$ and

$$\begin{aligned}\mathrm{Ker}(\phi) &= \big\{a \in G \big| C_a = I\big\} = \big\{a \in G \big| axa^{-1} = x \text{ for all } x \in G\big\} \\ &= \big\{a \in G \big| ax = xa \text{ for all } x \in G\big\} = Z(G)\end{aligned}$$

and so $Z(G) \trianglelefteq G$ with $G\big/Z(G) \cong \mathrm{Inn}(G)$.

5.22 Definition: Let $H \leq G$. The **centralizer** of H in G is the set

$$C(H) = C_G(H) = \big\{a \in G \big| ax = xa \text{ for all } x \in H\big\}$$

and the **normalizer** of H in G is the set

$$N(H) = N_G(H) = \big\{a \in G \big| aH = Ha\big\}\,.$$

5.23 Theorem: *(The Normalizer/Centralizer Theorem) Let $H \leq G$. Then $C(H) \trianglelefteq N(H)$ and $N(H)\big/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.*

Proof: The proof is left as an exercise.

5.24 Theorem: *(The Characterization of Internal Direct Products) Let G be a group. Let $H \trianglelefteq G$ and $K \trianglelefteq G$. Suppose that $H \cap K = \{e\}$ and that $G = HK = \big\{hk \big| h \in H, k \in K\big\}$. Then $G \cong H \times K$.*

Proof: Define $\phi : H \times K \to G$ by $\phi(h,k) = hk$. The map ϕ is a group homomorphism since for $h_1, h_2 \in H$ and $k_1, k_2 \in K$ we have

$$\begin{aligned}\phi\big((h_1,k_1)(h_2,k_2)\big) &= \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1{k_1}^{-1}h_2k_1{h_2}^{-1}h_2k_2 \\ &= h_1k_1eh_2k_2 = \phi(h_1,k_1)\phi(h_2,k_2),\end{aligned}$$

where we used the fact that the element ${k_1}^{-1}h_2k_1{h_2}^{-1}$ lies in both H and K (it lies in H since $H \trianglelefteq G$ so that ${k_1}^{-1}h_2k_1 \in H$, and it lies in K since $K \trianglelefteq G$ so that $h_2k_1{h_2}^{-1} \in K$), and we have $H \cap K = \{e\}$. The map ϕ is surjective since $G = HK$ so that every element in G is of the form $hk = \phi(h,k)$ for some $h \in H$, $k \in K$, and the map ϕ is injective since for $h \in H$ and $k \in K$ we have $\phi(h,k) = e \Longrightarrow hk = e \Longrightarrow h = k^{-1} \Longrightarrow h, k \in H \cap K \Longrightarrow h = k = e$, since $H \cap K = \{e\}$.

5.25 Theorem: (*The Classification of Groups of Order 2p*) *Let p be prime. Then (up to isomorphism) the distinct groups of order $2p$ are $\mathbf{Z}_{2p}$ and D_p.*

Proof: Let G be a group with $|G| = 2p$. Suppose that $G \not\cong \mathbf{Z}_{2p}$, so G is not cyclic. By Lagrange's Theorem, each element $a \in G$ has order $|a| = 1, 2, p$ or $2p$. Since G is not cyclic, no element has order $2p$ so every non-identity element in G has order 2 or p.

Suppose first that every non-identity element has order 2. Note that G must be abelian since for all $a, b \in G$ we have $a^2 = b^2 = (ba)^2 = e$ and so $ab = b^2aba^2 = b(ba)^2a = ba$. Fix two distinct non-identity elements $a, b \in G$ and consider the set $H = \{e, a, b, ab\}$. Note that H is closed under the operation and under inversion (since $a^2 = b^2 = e$ and $ab = ba$) and so $H = \langle a, b\rangle \leq G$. By Lagrange's Theorem, we have $|H|\big||G|$, that is $4\big|2p$, and so we must have $p = 2$ and so $|G| = 4 = |H|$, and so $G = H \cong {\mathbf{Z}_2}^2 \cong D_2$.

Now suppose that some non-identity element has order p with $p \neq 2$. Choose $a \in G$ with $|a| = p$. Choose $b \notin \langle a\rangle$. Note that since $\langle a\rangle = p$ and $|G| = 2p$, there are exactly two cosets of $\langle a\rangle$ in G, namely $\langle a\rangle$ and $b\langle a\rangle$, and G is the disjoint union $G = \langle a\rangle \cup b\langle a\rangle$. Note that $b^2\langle a\rangle \neq b\langle a\rangle$ since $b = b^{-1}b^2 \notin \langle a\rangle$, and so we must have $b^2\langle a\rangle = \langle a\rangle$ and hence $b^2 \in \langle a\rangle$. Note that $|b| \neq p$, since if we had $b^p = e$ then (since $p+1$ is even) we would have $b = b^{p+1} \in \langle b^2\rangle \subseteq \langle a\rangle$, and so $|b| = 2$. Similarly, we have $|x| = 2$ for every $x \notin \langle a\rangle$. Consider the element ab. Note that $ab \notin \langle a\rangle = a\langle a\rangle$ since $b = a^{-1}ab \notin \langle a\rangle$, and so we have $|ab| = 2$. Thus $abab = e$ and so $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{p-1}$

We have shown that G is the disjoint union $G = \langle a\rangle \cup b\langle a\rangle$, so we have

$$G = \left\{e, a, a^2, \cdots, a^{p-1}, b, ba, ba^2, \cdots, ba^{p-1}\right\}$$

with the listed elements distinct. Since $ab = ba^{-1}$, we have $a^2b = aba^{-1} = ba^{-2}$ and $a^3b = aba^{-2} = ba^{-3}$ and so on so that $a^kb = ba^{-k}$. This determines the operation on G completely. Indeed we have

$$a^k \cdot a^l = a^{k+l} \ , \ a^k \cdot ba^l = ba^{l-k} \ , \ ba^k \cdot a^l = ba^{k+l} \ , \ ba^k \cdot ba^l = a^{l-k} \, .$$

Compare this to the operation in $D_p = \left\{I, R_1, \cdots, R_{p-1}, F_0, F_1, \cdots, F_{p-1}\right\}$ given by

$$R_k \cdot R_l = R_{k+l} \ , \ R_k \cdot F_{-l} = F_{-(l-k)} \ , \ F_{-k}R_l = F_{-(k+l)} \ , \ F_{-k}F_{-l} = F_{-(l-k)} \, .$$

We see that the map $\phi : G \to D_p$ given by $\phi(a^k) = R_k$ and $\phi(ba^l) = F_{-l}$ is an isomorphism.

5.26 Theorem: (*The Classification of Groups of Order p^2*) *Let p be prime. Then (up to isomorphism) the distinct groups of order p^2 are $\mathbf{Z}_{p^2}$ and $\mathbf{Z}_p \times \mathbf{Z}_p$.*

Proof: Let G be a group with $|G| = p^2$. Suppose that $G \not\cong \mathbf{Z}_{p^2}$ so that G is not cyclic. Each $a \in G$ has order $|a| = 1, p$ or p^2. Since G is not cyclic, every non-identity element has order p.

Let a be a non-identity element in G. We claim that $\langle a \rangle \trianglelefteq G$. Suppose, for a contradiction, that $\langle a \rangle \ntrianglelefteq G$. Choose $x \in G$ and $a^k \in \langle a \rangle$ so that $x\, a^k x^{-1} \notin \langle a \rangle$. This implies that $xax^{-1} \notin \langle a \rangle$ since $x\, a^k x^{-1} = (xax^{-1})^k$. Since $xax^{-1} \neq e$ we have $\left| xax^{-1} \right| = p$. Note that $\langle a \rangle \cap \langle\, xax^{-1} \rangle = \{e\}$ because $\langle a \rangle \cap \langle\, xax^{-1} \rangle$ is a proper subgroup of $\langle a \rangle \cong \mathbf{Z}_p$. It follows that the cosets

$$e\langle\, xax^{-1} \rangle, a\langle\, xax^{-1} \rangle, a^2\langle\, xax^{-1} \rangle, \cdots, a^{p-1}\langle\, xax^{-1} \rangle$$

are distinct since if $a^k\langle xax^{-1} \rangle = a^l\langle xax^{-1} \rangle$ then $a^{l-k} \in \langle xax^{-1} \rangle$ so $a^{l-k} \in \langle a \rangle \cap \langle xax^{-1} \rangle$ and hence $a^{l-k} = e$. Thus G is the disjoint union of these p cosets. In particular, the element x^{-1} lies in some coset. But this is not possible since if $x^{-1} \in a^k\langle\, xax^{-1} \rangle$ with say $x^{-1} = a^k x\, a^l x^{-1}$, then we would have $a^k x\, a^l = e$ and hence $x = a^{-k-l} \in \langle a \rangle$. This proves the claim.

Fix a non-identity element $a \in G$ and choose an element $b \in G$ with $b \notin \langle a \rangle$. Then we have $\langle a \rangle \trianglelefteq G$ and $\langle b \rangle \trianglelefteq G$. As above, we have $\langle a \rangle \cap \langle b \rangle = \{e\}$ (since $\langle a \rangle \cap \langle b \rangle$ is a proper subgroup of $\langle a \rangle \cong \mathbf{Z}_p$), and as above this implies that the cosets

$$e\langle b \rangle\,,\ a\langle b \rangle\,,\ a^2\langle b \rangle\,,\ \cdots\,,\ a^{p-1}\langle b \rangle$$

are distinct (since if $a^k\langle b \rangle = a^l\langle b \rangle$ then $a^{l-k} \in \langle b \rangle$ hence $a^{l-k} \in \langle a \rangle \cap \langle b \rangle = \{e\}$). Thus every element of G is of the form $a^i b^j$, that is $G = \langle a \rangle\langle b \rangle$. By the Characterization of Internal Direct Products, we have $G \cong \langle a \rangle \times \langle b \rangle \cong \mathbf{Z}_p \times \mathbf{Z}_p$.

5.27 Definition: A group G is **simple** when its only normal subgroups are $\{e\}$ and G.

5.28 Theorem: F*or $n \geq 5$, the alternating group A_n is simple.*

Proof: Let $H \trianglelefteq A_n$. We shall show that $H = A_n$. We consider 5 cases. Case 1: suppose first that H contains a 3-cycle, say $(abc) \in H$. Then for any $k \neq a, b, c$ we have $(abk) = (ab)(ck)\,(abc)^2(ck)(ab) \in H$ It follows that $A_n = H$ because A_n is generated by the 3-cycles of the form (abk) with $k \neq a, b$ (as shown in Example 3.25). Case 2: suppose that H contains an element α which, when written in cycle notation, has a cycle of length $r \geq 4$, say $\alpha = (a_1a_2a_3 \cdots a_r)\beta \in H$. Then $(a_1a_3a_r) = \alpha^{-1}(a_1a_2a_3)\alpha(a_1a_2a_3)^{-1} \in H$ and so $H = A_n$ by Case 1. Case 3: suppose that H contains an element α which, when written in cycle notation, has at least two 3-cycles, say $\alpha = (a_1a_2a_3)(a_4a_5a_6)\beta \in H$. Then we have $(a_1a_4a_2a_6a_3) = \alpha^{-1}(a_1a_2a_4)\alpha(a_1a_2a_4)^{-1} \in H$ and so $H = A_n$ by Case 2. Case 4: suppose that H contains an element α which, when written in cycle notation, is a product of one 3-cycle and some 2-cycles, say $\alpha = (a_1a_2a_3)\beta \in H$ where β is a product of disjoint 2-cycles so that $\beta^2 = e$. Then $(a_1a_3a_2) = \alpha^2 \in H$ and so $H = A_n$ by Case 1. Case 5: suppose that H contains an element α which, when written in cycle notation, is a product of 2-cycles, say $\alpha = (a_1a_2)(a_3a_4)\beta \in H$. Then $(a_1a_3)(a_2a_4) = \alpha^{-1}(a_1a_2a_3)\alpha(a_1a_2a_3)^{-1} \in H$. Let $\gamma = (a_1a_3)(a_2a_4)$ and choose b distinct from a_1, a_2, a_3, a_4. Then $(a_1a_3b) = \gamma(a_1a_2b)\gamma(a_1a_3b)^{-1} \in H$ and so $H = A_n$ by Case 1.

.

Chapter 6. Group Actions on Sets

6.1 Definition: Let G be a group. A **representation** of G is a group homomorphism $\rho : G \to \text{Perm}(S)$ for some set S. A representation $\rho : G \to \text{Perm}(S)$ is called **faithful** when it is injective.

6.2 Remark: Given a faithful representation $\rho : G \to \text{Perm}(S)$, we sometimes identify the group G with its isomorphic image $\rho(G)$, which is a group of permutations of S.

6.3 Definition: Let G be a group and let S be a set. A **group action** of G on S is a map $* : G \times S \to S$, where for $a \in G$ and $x \in S$ we write $*(a, x)$ as $a * x$ or simply as ax, such that

(1) $ex = x$ for all $x \in S$, and
(2) $(ab)x = a(bx)$ for all $a, b \in G$ and all $x \in S$.

6.4 Note: Given a group G and a set S, here is a natural bijective correspondence between representations $\rho : G \to \text{Perm}(S)$ and group actions $* : G \times S \to S$. The representation ρ and its corresponding group action $*$ determine one another by the formula

$$a * x = \rho(a)(x) \text{ for all } a \in G, x \in S\,.$$

As an exercise, verify that given a representation ρ, this formula defines a group action $*$, and conversely that given a group action $*$, the formula defines a representation ρ.

6.5 Definition: Suppose that a group G acts on a set S. The group action is called **faithful** when the corresponding representation is faithful.

6.6 Example: When a group G acts on itself by its own operation, so $a*x = ax = L_a(x)$, the corresponding representation $\rho : G \to \text{Perm}(G)$ is given by $\rho(a) = L_a$. This is the map that was used in the proof of Cayley's Theorem. The representation is faithful, so it gives an isomorphism from G to its image $\rho(G) \leq \text{Perm}(G)$.

6.7 Example: When a group G acts on itself by conjugation, so $a * x = axa^{-1} = C_a(x)$, the corresponding representation $\rho : G \to \text{Perm}(G)$ is given by $\rho(a) = C_a$. This is the homomorphism considered in Example 5.21 with $\text{Ker}(\phi) = Z(G)$ and $\text{Image}(\phi) = \text{Inn}(G)$ giving the isomorphism $G/Z(G) \cong \text{Inn}(G)$.

6.8 Example: When R is a commutative ring with 1 and the group $GL_n(R)$ acts on R^n by matrix multiplication, so that $A * x = Ax = L_A(x)$, the corresponding representation $\rho : GL_n(R) \to \text{Perm}(R^n)$ is given by $\rho(A) = L_A$ (so ρ sends the matrix A to the linear map L_A given by $L_A(x) = Ax$). The representation is faithful, so its gives an isomorphism from $GL_n(R)$ (which is a set of invertible matrices) to its image (which is a set of invertible linear maps).

6.9 Definition: Let G be a group which acts on a set S. For $a \in G$ we define the **fixed set** of a in S to be the set

$$\text{Fix}(a) = \big\{x \in S \big| ax = x\big\} \subseteq S\,.$$

For $x \in S$ we define the **orbit** of x in S to be the set

$$\text{Orb}(x) = \big\{ax \big| a \in G\big\} \subseteq S\,.$$

Verify that for $x, y \in S$ we have $y \in \text{Orb}(x) \iff \text{Orb}(x) = \text{Orb}(y)$ so, for the equivalence relation on S given by $x \sim y \iff \text{Orb}(x) = \text{Orb}(y)$, the equivalence class of x is equal to the orbit of x. The set of distinct orbits is denoted by S/G so we have

$$S/G = \left\{ \text{Orb}(x) \middle| x \in S \right\}.$$

For $x \in S$ we define the **stabilizer** of x in G to be the subgroup

$$\text{Stab}(x) = \left\{ a \in G \middle| ax = x \right\} \leq G.$$

Note that Stab(x) $\leq G$ because $ex = x$, if $ax = x$ and $bx = x$ then $(ab)x = a(bx) = ax = x$, and if $ax = x$ then $x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}x$.

6.10 Theorem: (*The Orbit-Stabilizer Theorem*) *Let G be a group which acts on a set S. Then for all $x \in S$ we have*

$$|G| = \left|\text{Orb}(x)\right| \left|\text{Stab}(x)\right|.$$

Proof: Let $x \in S$. We shall show that $\Big|\text{Orb}(x)\Big| = \Big|G/\text{Stab}(x)\Big|$. Write $H = \text{Stab}(x)$. Define a map $\Phi : G/H \to \text{Orb}(x)$ by $\Phi(aH) = ax$. Then Φ is well-defined because for $a, b \in G$ we have $aH = bH \implies b^{-1}a \in H \implies b^{-1}a\,x = x \implies ax = bx$, Φ is injective because for $a, b \in G$ we have $ax = bx \implies b^{-1}a\,x = x \implies b^{-1}a \in H \implies aH = bH$, and the map Φ is clearly surjective.

6.11 Example: Consider D_6 as a subgroup of S_6. Find Orb(1) and Stab(1).

6.12 Example: Let G be the rotation group of a cube Q. Label the vertices of the cube by elements of $S = \{1, 2, \cdots, 6\}$, think of the elements of G as permutations of S and hence identify G with a subgroup of S_6. Find $\left|\text{Orb}(1)\right|$ and $\left|\text{Stab}(1)\right|$ and hence find $|G|$.

6.13 Example: (The Class Equation) When G acts on itself by conjugation, so that $a * x = axa^{-1}$, for $a, x \in G$, we have $\text{Orb}(x) = \left\{ axa^{-1} \middle| a \in G \right\} = Cl(x)$, so the orbit of x is the conjugacy class of x in G, and we have $\text{Stab}(x) = \left\{ a \in G \middle| axa^{-1} = x \right\} = C(x)$, so the stabilizer of x is the centralizer of x in G. Suppose that G is a finite group. Say G has n distinct conjugacy classes, and choose one element $x_i \in G$ from each class so that we have $G = \bigcup_{i=1}^{n} \text{Orb}(x_i)$. By the Orbit-Stabilizer Theorem, $\left|\text{Orb}(x_i)\right| = \frac{|G|}{|C(x_i)|} = \left|G/C(x_i)\right|$ and so

$$|G| = \sum_{i=1}^{n} \left|G/C(x_i)\right|.$$

This equation is called the **class equation** for G.

6.14 Example: Let S be the set of all subgroups of a group G. Let G act on S by conjugation, so $a * H = C_a(H) = aHa^{-1}$, where $a \in G$ and $H \leq G$. For $H \in S$, that is $H \leq G$, we have

$$\begin{aligned} \text{Stab}(H) &= \left\{ a \in G \middle| aHa^{-1} = H \right\} = \left\{ a \in G \middle| aH = Ha \right\} = N_G(H), \\ \text{Orb}(H) &= \left\{ aHa^{-1} \middle| a \in G \right\} = \text{Cl}(H), \end{aligned}$$

where $N_G(H)$ is the normalizer of H in G and $\text{Cl}(H)$ is the conjugacy class of H in G, that is the set of all subgroups conjugate to H in G.

6.15 Theorem: (*Cauchy's Theorem*) *Let G be a finite group. Let p be a prime divisor of $|G|$. Then G contains an element of order p. Indeed*

$$\Big|\big\{a \in G\big||a| = p\big\}\Big| = p - 1 \bmod p(p-1)\,.$$

Proof: Let n be the number of elements of order p in G, that is $n = \big|\{a \in G\big||a| = p\}\big|$. Recall that $n = 0 \mod (p-1)$ (indeed n is equal to $(p-1)$ times the number of cyclic subgroups of order p in G because each of these subgroups has $\phi(p) = p-1$ generators). Let $S = \big\{(x_1, x_2, \cdots, x_p) \in G^p \big| x_1 x_2 \cdots x_p = e\big\}$. Note that $|S| = |G|^{p-1}$ since to get $(x_1, x_2, \cdots, x_p) \in S$ we can choose $x_1, x_2, \cdots, x_{p-1}$ arbitrarily and then x_p must be given by $x_p = (1_1 x_2 \cdots x_{p-1})^{-1}$. Note that $\mathbf{Z}_p$ acts on S by cyclic permutation, that is by

$$k * (x_1, x_2, \cdots, x_p) = (x_{1+k}, x_{2+k}, \cdots, x_p, x_1, \cdots, x_k)$$

since if $x_1 x_2 \cdots x_p = e$ then $x_1 x_2 \cdots x_k = (x_{k+1} \cdots x_p)^{-1}$ so $x_{1+k} x_{2+k} \cdots x_p x_1 \cdots x_k = e$. For $x = (x_1, x_2, \cdots, x_p) \in S$, by the Orbit/Stabilizer Theorem $\big|\mathrm{Orb}(x)\big|$ divides $|\mathbf{Z}_p| = p$ so that $\big|\mathrm{Orb}(x)\big| \in \{1, p\}$, so we have

$$\Big|\mathrm{Orb}(x)\Big| = \begin{cases} 1 \text{ , if } x = (a, a, \cdots, a) \text{ for some } a \in G, \text{ and} \\ p \text{ , otherwise.} \end{cases}$$

Since S is the disjoint union of the orbits, we have $|S| = k + pl$ where k is the number of orbits of size 1 and l is the number of orbits of size p. Note that k is equal to the number of elements $a \in G$ with $a^p = 1$, and so $k = 1 + n$. Since $|S| = |G|^{p-1} = 0 \mod p$ we have $n = k - 1 = |S| - pl - 1 = -1 \mod p$. Since $n = -1 = p - 1 \bmod p$ and $n = 0 = p - 1 \bmod (p-1)$, we have $n = p - 1 \mod p(p-1)$ by the Chinese Remainder Theorem.

6.16 Theorem: Let *G be a finite group and let $H \leq G$. Suppose that $|G/H| = p$, where p is the smallest prime divisor of $|G|$. Then $H \trianglelefteq G$.*

Proof: Let $S = G/H = \big\{aH\big|a \in G\big\}$. Since $|S| = p$ we have $\mathrm{Perm}(S) \cong S_p$. Let G act on S by left multiplication, so we have $a * (bH) = abH$ for $a, b \in G$. Let $\rho : G \to \mathrm{Perm}(S)$ be the associated representation, so $\rho(a)(bH) = abH$. Let

$$K = \mathrm{Ker}(\rho) = \big\{a \in G\big|abH = bH \text{ for all } b \in G\big\} \trianglelefteq G\,.$$

Note that $K \leq H$ because $a \in K \implies aeH = eH \implies a \in H$. Since $K \trianglelefteq G$ (it is the kernel of a homomorphism) and $K \leq H$, we also have $K \trianglelefteq H$. By the First Isomorphism Theorem, we have $G/K \cong \rho(G) \leq \mathrm{Perm}(S) \cong S_p$. By Lagrange's Theorem $|G/K|$ divides $|S_p| = p!$. By another application of Lagrange's Theorem, $|G/K|$ also divides $|G|$. Since $|G/K|\,\big|\,|G|$ and p is the smallest prime factor of $|G|$, $|G/K|$ has no prime factors less than p. Since $|G/K|\,\big|\,p!$, we must have $|G/K| = 1$ or p. Since $|G/K| = |G/H|\,|H/K| = p|H/K|$ we have $|G/K| = p$ and $|H/K| = 1$. Thus in fact $H = K \trianglelefteq G$.

6.17 Theorem: (*The Burnside or Cauchy-Frobenius Lemma*) *Let G be a finite group which acts on a set S. Then*

$$|G|\,\big|S/G\big| = \sum_{a\in G} \big|\mathrm{Fix}(a)\big|\,.$$

Proof: Let $T = \big\{(a,x)\big| a\in G, x\in S, ax = x\big\}$. Then we have

$$|T| = \sum_{a\in G} \big|\{x\in S|ax=x\}\big| = \sum_{a\in G}\big|\mathrm{Fix}(a)\big|$$

and we have

$$\begin{aligned}|T| &= \sum_{x\in S}\big|\{a\in G\big|ax=x\}\big| = \sum_{x\in S}\big|\mathrm{Stab}(x)\big| = \sum_{x\in S}\frac{|G|}{|\mathrm{Orb}(x)|}\\ &= |G|\sum_{x\in S}\frac{1}{|\mathrm{Orb}(x)|} = |G|\sum_{A\in S/G}\sum_{x\in A}\frac{1}{|A|} = |G|\sum_{A\in S/G} 1 = |G|\big|S/G\big|\,.\end{aligned}$$

6.18 Example: In how many ways (up to symmetry under the action of D_6) can we colour the vertices of the regular hexagon C_6 using 3 colours?

Solution: Let S be the set of possible colourings without considering symmetry under D_6, and note that $|S| = 3^6$. The natural action of D_6 on C_6 induces an action of D_6 on S. We make a table showing $\big|\mathrm{Fix}(A)\big|$ for each $A\in D_6$.

A	# of such A	$\big\|\mathrm{Fix}(A)\big\|$
I	1	3^6
R_3	1	3^3
R_2, R_4	2	3^2
R_1, R_5	2	3^1
F_0, F_2, F_4	3	3^4
F_1, F_3, F_5	3	3^3

The number of colourings up to D_6 symmetry is equal to the number of orbits, which is

$$\big|S/D_6\big| = \frac{1}{|D_6|}\sum_{A\in D_6}\big|\mathrm{Fix}(A)\big| = \tfrac{1}{12}\big(3^6+3^3+2\cdot 3^2+2\cdot 3^1+3\cdot 3^4+3\cdot 3^2\big) = 92\,.$$

6.19 Example: Let G be the rotation group of a cube Q. In how many ways (up to symmetry under the action of G) can we colour the 8 vertices of Q using 2 colours?

Solution: The solution is left as an exercise.

.

Chapter 7. The Classification of Finite Abelian Groups

7.1 Note: In this chapter we will use additive notation for all abelian groups.

7.2 Definition: A **free abelian group** of **rank** n is an abelian group isomorphic to $\mathbf{Z}^n$.

7.3 Theorem: *The rank of a free abelian group G is unique, that is if $G \cong \mathbf{Z}^n$ and $G \cong \mathbf{Z}^m$ then $n = m$.*

Proof: Suppose that $G \cong \mathbf{Z}^n$ and $G \cong \mathbf{Z}^m$ so that $\mathbf{Z}^n \cong \mathbf{Z}^m$. Let $\phi : \mathbf{Z}^n \to \mathbf{Z}^m$ be an isomorphism. Note that ϕ sends $2\mathbf{Z}^n$ bijectively to $2\mathbf{Z}^m$, so it induces an isomorphism $\psi : \mathbf{Z}^n/2\mathbf{Z}^n \to \mathbf{Z}^m/2\mathbf{Z}^m$ given by $\psi(k+2\mathbf{Z}^n) = \phi(k)+2\mathbf{Z}^m$. Also note that $\mathbf{Z}_n/2\mathbf{Z}^n \cong {\mathbf{Z}_2}^n$ and $\mathbf{Z}^m/2\mathbf{Z}^m \cong \mathbf{Z}^{2m}$, so we have ${\mathbf{Z}_2}^n \cong {\mathbf{Z}_2}^m$. Thus $2^n = \left|{\mathbf{Z}_2}^n\right| = \left|{\mathbf{Z}_2}^m\right| = 2^m$ so $n = m$.

7.4 Definition: Let G be an additive abelian group. Let $u_1, u_2, \cdots, u_\ell \in G$ be distinct and let $U = \{u_1, u_2, \cdots, u_\ell\}$. A **linear combination** of elements in U (over $\mathbf{Z}$) is an element of G of the form

$$a = t_1u_1 + t_2u_2 + \cdots t_\ell u_\ell \text{ for some } t_i \in \mathbf{Z}\,.$$

The **span** of U (over $\mathbf{Z}$) is the set of all linear combinations, that is

$$\mathrm{Span}_{\mathbf{Z}}(U) = \langle U\rangle = \left\{t_1u_1 + t_2u_2 + \cdots + t_\ell u_\ell \,\middle|\, \text{each } t_i \in \mathbf{Z}\right\}$$

We say that U is **linearly independent** (over $\mathbf{Z}$) when for all $t_i \in \mathbf{Z}$,

$$\text{if } t_1u_1 + t + 2u_2 + \cdots + t_\ell u_\ell = 0 \text{ then every } t_i = 0.$$

We say that U is a **basis** for G (over $\mathbf{Z}$) when U is linearly independent and $\mathrm{Span}_{\mathbf{Z}}(U) = G$. An **ordered basis** for G (over $\mathbf{Z}$) is an ordered n-tuple $(u_1, u_2, \cdots, u_n)$ of distinct elements $u_i \in G$ such that $U = \{u_1, u_2, \cdots, u_n\}$ is a basis for G (over $\mathbf{Z}$). Note that if U is a basis for G over $\mathbf{Z}$, every element in G can be written uniquely (up to the order of the terms) as a linear combination of elements in U over $\mathbf{Z}$.

7.5 Example: Let $e_k = (0, \cdots, 0, 1, 0, \cdots, 0) \in \mathbf{Z}^n$ where the 1 is in the k^{th} position. Then $\{e_1, e_2, \cdots, e_n\}$ is a basis, which we call the **standard basis** for $\mathbf{Z}^n$ over $\mathbf{Z}$.

7.6 Theorem: *Let G be an abelian group. Then G is a free abelian group of rank n if and only if G has a basis over $\mathbf{Z}$ with n-elements.*

Proof: Suppose that $G \cong \mathbf{Z}^n$ and let $\phi : \mathbf{Z}^n \to G$ is a group isomorphism. Verify that the set $U = \left\{\phi(e_1), \phi(e_2), \cdots, \phi(e_n)\right\}$ is a basis for G over $\mathbf{Z}$. Conversely, suppose that $U = \{u_1, u_2, \cdots, u_n\}$ is a basis for G over $\mathbf{Z}$. Verify that the map $\phi : \mathbf{Z}^n \to G$ given by

$$\phi(t_1, t_2, \cdots, t_n) = \left(t_1u_1 + t_2u_2 + \cdots + t_nu_n\right)$$

is a group isomorphism.

7.7 Theorem: *Let $U = (u_1, u_2, \cdots, u_n)$ be an ordered basis over $\mathbf{Z}$ for the free abelian group G. Then we can perform any of the following operations to the elements in the basis to obtain a new ordered basis for G over $\mathbf{Z}$.*

(1) $u_i \leftrightarrow u_j$: interchange two elements,
(2) $u_i \mapsto \pm u_i$: multiply an element by ± 1,
(3) $u_i \mapsto u_i + ku_j$: add an integer multiple of one element to another.

Proof: The proof is left as an exercise.

7.8 Theorem: (*Subgroups and Quotient Groups of* $\mathbf{Z}^n$) *Let G be a free abelian group of rank n. Let $H \leq G$. Then H is a free abelian group of rank r for some $0 \leq r \leq n$ and*

$$G/H \cong \mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_r} \times \mathbf{Z}^{n-r}$$

for some $d_i \in \mathbf{Z}^+$ with $d_1 \big| d_2, d_2 \big| d_3, \cdots, d_{r-1} \big| d_r$.

Proof: We claim that there exists a basis $\{u_1, u_2, \cdots, u_n\}$ for G and there exist r and $d_1, d_2, \cdots, d_r$ with $0 \leq r \leq n$ and $d_1 \big| d_2, d_2 \big| d_3, \cdots, d_{r-1} \big| d_r$ such that $\{d_1 u_1, d_2 u_2, \cdots, d_r u_r\}$ is a basis for H. Once we have proven this claim, it is not hard to check that the map $\phi : G \to \mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_r} \times \mathbf{Z}^{n-r}$ given by $\phi(t_1 u_1 + \cdots + t_n u_n) = (t_1, \cdots, t_n)$ is a surjective group homomorphism with $\text{Ker}(\phi) = H$, so that

$$G/H \cong \mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_r} \times \mathbf{Z}^{n-r}$$

by the First Isomorphism Theorem.

When $n = 1$ so $G \cong \mathbf{Z}$, we have $G = \langle a \rangle = \text{Span}_{\mathbf{Z}}\{a\}$ for some $a \in G$ with $|a| = \infty$, and $H = \langle ka \rangle$ for some $k \geq 0$. If $k = 0$ so $H = \{0\}$ (so the empty set is a basis for H), the claim holds with $u_1 = a$ and $r = 0$. If $k > 0$, the claim holds with $u_1 = a$, $r = 1$, $d_1 = k$.

Let $n \geq 2$ and suppose, inductively, that the claim holds for free abelian groups of rank $n - 1$. Let $G \cong \mathbf{Z}^n$ with $H \leq G$. If $H = \{0\}$ (so the empty set is a basis for H), the claim holds with $r = 0$. Suppose that $H \neq \{0\}$. Let T be the set of all coefficients t_i in all linear combinations $a = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n$ over all elements $a \in H$ and all possible choices of basis $\{v_1, v_2, \cdots, v_n\}$ for G. Let $d_1 \in \mathbf{Z}^+$ be the smallest positive integer in T. Choose a basis $\{v_1, v_2, \cdots, v_n\}$ for G and an element $a = d_1 v_1 + t_2 v_2 + t_3 v_3 + \cdots + t_n v_n \in H$. Note that $d_1 \big| t_i$ for all $i \geq 2$ because if we write $t_i = q_i d_1 + r_i$ with $0 \leq r_i < d_i$ then

$$\begin{aligned} a &= d_1 v_1 + (q_2 d_1 + r_2) v_2 + (q_3 d_1 + r_3) v_2 + \cdots + (q_n d_1 + r_n) v_n \\ &= d_1 (v_1 + q_2 v_2 + q_3 v_3 + \cdots + q_n v_n) + r_2 v_2 + r_3 v_3 + \cdots + r_n v_n \end{aligned}$$

and so each $r_i = 0$ by the choice of d_1 since $\{v_1 + \sum q_i v_i \, , v_2, v_3, \cdots, v_n\}$ is a basis for G. Let $u_1 = v_1 + \sum q_i v_i$ so that $\{u_1, v_2, v_3, \cdots, v_n\}$ is a basis for G and $a = d_1 u_1 \in H$.

Let $G_0 = \text{Span}\{v_2, v_3, \cdots, v_n\}$ and let $H_0 = H \cap G_0$. Let $a \in H$. Since $\{u_1, v_2, \cdots, v_n\}$ is a basis for G, we know that a can be written uniquely in the form $a = t_1 u_1 + t_2 v_2 + \cdots t_n v_n$. Note that we must have $d_1 \big| t_1$ because if we write $t_1 = q_1 d_1 + r_1$ with $0 \leq r_1 < d_1$ then since $a = (q_1 d_1 + r_1) u_1 + t_2 v_2 + \cdots + t_n v_n \in H$, we have $r_1 u_1 + t_2 v_2 + \cdots + t_n v_n = a - q_1 d_1 u_1 \in H$, and so $r_1 = 0$ by the choice of d_1. Also note that for $b = a - t_1 u_1 = t_2 v_2 + \cdots + t_n v_n$ we have $b \in \text{Span}\{v_2, \cdots, v_n\} = G_0$ and since $d_1 \big| t_1$ and $d_1 u_1 \in H$ we have $t_1 u_1 \in H$, and so $b \in H \cap G_0 = H_0$. Thus every $a \in H$ can be written uniquely as $a = t_1 u_1 + b$ with $d_1 \big| t_1$ and $b \in H_0$.

By the induction hypothesis, we can find a basis $\{u_2, u_3, \cdots, u_n\}$ for G_0 and we can find r and $d_2, d_3, \cdots, d_n$ with $1 \leq r \leq n$ and $d_2 \big| d_3, d_3 \big| d_4, \cdots d_{r-1} \big| d_r$ such that $\{d_2 u_2, \cdots, d_r u_r\}$ is a basis for H_0. Since each $a \in H$ can be written uniquely as $a = t_1 u_1 + b$ with $d_1 \big| t_1$ and $b \in H_0 = \text{Span}\{d_2 u_2, \cdots, d_n u_n\}$, it follows that $\{d_1 u_1, d_2 u_2, \cdots, d_n u_n\}$ is a basis for H. Finally, note that we must have $d_1 \big| d_2$ because if we write $d_2 = q_2 d_1 + r_2$ with $0 \leq r_2 < d_1$ then we have $d_1 u_1 + d_2 u_2 \in H$, so that $d_1 u_1 + (q_2 d_1 + r_2) u_2 \in H$, hence $d_1(u_1 + q_2 u_2) + r_2 u_2 \in H$ and so $r_2 = 0$ by the choice of d_1, since $\{u_1 + q_2 u_2, u_2, \cdots, u_n\}$ is another basis for G.

7.9 Theorem: (*The Classification of Finite Abelian Groups) Every finite abelian group is isomorphic to a unique group of the form*

$$\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_l}$$

for some integer $l \geq 0$ and some integers n_i with $2 \leq n_1$, $n_1 \big| n_2, n_2 \big| n_3, \cdots, n_{l-1} \big| n_l$.

Alternatively, every finite abelian group is isomorphic to a unique group of the form

$$\mathbf{Z}_{{p_1}^{k_1}} \times \mathbf{Z}_{{p_2}^{k_2}} \times \cdots \times \mathbf{Z}_{{p_m}^{k_m}}$$

for some integer $m \geq 0$ and some primes p_i with $p_1 \leq p_2 \leq \cdots \leq p_m$ and some positive integers k_i with $k_i \leq k_{i+1}$ whenever $p_i = p_{i+1}$.

Proof: First we prove that every finite abelian group is isomorphic to a group of the first form. Let G be a finite additive abelian group, say $|G| = n$ and $G = \{a_1, a_2, \cdots .a_n\}$. Define $\phi : \mathbf{Z}^n \to G$ by $\phi(t_1, t_2, \cdots, t_n) = t_1 a_1 + \cdots + t_n a_n$. Then ϕ is a group homomorphism since G is abelian, and ϕ is clearly onto. By the First Isomorphism Theorem we have $G \cong \mathbf{Z}^n \big/ \mathrm{Ker}(\phi)$. By the previous theorem,

$$G \cong \mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \cdots \times \mathbf{Z}_{d_r} \times \mathbf{Z}^{n-r}$$

for some integers r and $d_1, d_2, \cdots, d_r$ with $0 \leq r \leq n$ and $d_1 \big| d_2, d_2 \big| d_3, \cdots, d_{r-1} \big| d_r$. Since G is finite we must have $r = n$. Say $d_1 = d_2 = \cdots d_k = 1$ and $d_{k+1} > 1$. Then we have

$$G = \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_l}$$

as required, by taking $n_i = d_{k+i}$.

Next we describe a bijective correspondence between groups of the first form and groups of the second form. Given a group $G = \mathbf{Z}_{n_1} \times \cdots \times \mathbf{Z}_{n_l}$ of the first form, we can obtain an isomorphic group H of the second form as follows. For each $j = 1, 2, \cdots l$, decompose n_j into its prime factorization $n_j = \prod {p_{ji}}^{k_{ji}}$, replace the group $\mathbf{Z}_{n_j}$ by the isomorphic group $\prod \mathbf{Z}_{{p_{ji}}^{k_{ji}}}$, and then let H be the product of all the groups ${p_{ji}}^{k_{ji}}$ arranged in the required order. For example, for $G = \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_{12} \times \mathbf{Z}_{24} \times \mathbf{Z}_{720}$, we have

$$\begin{aligned} G &= \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_{12} \times \mathbf{Z}_{24} \times \mathbf{Z}_{720} \\ &\cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times (\mathbf{Z}_4 \times \mathbf{Z}_3) \times (\mathbf{Z}_8 \times \mathbf{Z}_3) \times (\mathbf{Z}_{16} \times \mathbf{Z}_9 \times \mathbf{Z}_5) \\ &\cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_{16} \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_9 \times \mathbf{Z}_5 = H\,. \end{aligned}$$

Conversely, given the group $H = \mathbf{Z}_{{p_1}^{k_1}} \times \cdots \times \mathbf{Z}_{{p_m}^{k_m}}$ of the second form, we can recover the group G of the first form as follows. First rewrite the list of (not necessarily distinct) primes $p_1, p_2, \cdots, p_m$ as $q_1, q_1, \cdots, q_1, q_2, q_2, \cdots, q_2, \cdots, q_r, q_r, \cdots, q_r$ where the q_i are distinct primes, where say q_i occurs s_i times in the list, and rewrite the list ${p_1}^{k_1}, \cdots, {p_m}^{k_m}$ in the form ${q_1}^{k_{11}}, \cdots, {q_1}^{k_{1,s_1}}, {q_2}^{k_{21}}, \cdots, {q_2}^{k_{2,s_2}}, \cdots, {q_r}^{k_{r1}}, \cdots, {q_r}^{k_{r,s_r}}$. Then let $s = \max\{s_1, s_2, \cdots, s_r\}$, and replace each of the products $\mathbf{Z}_{{q_i}^{k_{i1}}} \times \cdots \times \mathbf{Z}_{{q_i}^{k_{i,s_i}}}$ by the isomorphic product $\mathbf{Z}_{{q_i}^{l_{i1}}} \times \cdots \times \mathbf{Z}_{{q_i}^{l_{i,s}}}$ where $l_{i,1} = l_{i,2} = \cdots = l_{i,s-s_i} = 0$ and $l_{i,s-s_i+j} = k_{i,j}$ for $j = 1, 2, \cdots, s_i$. We then have

$$H = \prod_{i=1}^{r} \prod_{j=1}^{s} \mathbf{Z}_{{q_i}^{l_{ij}}} \cong \prod_{j=1}^{s} \prod_{i=1}^{r} \mathbf{Z}_{{q_i}^{l_{ij}}} \cong \prod_{j=1}^{s} \mathbf{Z}_{n_j} = G \text{ , where } n_j = \prod_{i=1}^{r} {q_i}^{l_{ij}} \,.$$

For example, for $H = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_9 \times \mathbf{Z}_9 \times \mathbf{Z}_{81} \times \mathbf{Z}_5 \times \mathbf{Z}_{25} \times \mathbf{Z}_7$ we have

$$\begin{aligned} H &= \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_9 \times \mathbf{Z}_9 \times \mathbf{Z}_{81} \times \mathbf{Z}_5 \times \mathbf{Z}_{25} \times \mathbf{Z}_7 \\ &\cong (\mathbf{Z}_1 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_8) \times (\mathbf{Z}_3 \times \mathbf{Z}_9 \times \mathbf{Z}_9 \times \mathbf{Z}_{81}) \\ &\qquad \times (\mathbf{Z}_1 \times \mathbf{Z}_1 \times \mathbf{Z}_5 \times \mathbf{Z}_{25}) \times (\mathbf{Z}_1 \times \mathbf{Z}_1 \times \mathbf{Z}_1 \times \mathbf{Z}_7) \\ &\cong (\mathbf{Z}_1 \times \mathbf{Z}_3 \times \mathbf{Z}_1 \times \mathbf{Z}_1) \times (\mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_1 \times \mathbf{Z}_1) \\ &\qquad \times (\mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_5 \times \mathbf{Z}_1) \times (\mathbf{Z}_8 \times \mathbf{Z}_{81} \times \mathbf{Z}_{25} \times \mathbf{Z}_7) \\ &\cong \mathbf{Z}_3 \times \mathbf{Z}_{18} \times \mathbf{Z}_{90} \times \mathbf{Z}_{113400} = G\,. \end{aligned}$$

You should convince yourself that the above two procedures give a bijective correspondence between groups of the two forms described in the statement of the theorem.

Finally, we show uniqueness for groups G of the second form. To do this, we shall show that the primes p_i and the exponents k_i are uniquely determined by the isomorphism class of the group G. Suppose that

$$G \cong \mathbf{Z}_{{p_1}^{k_1}} \times \mathbf{Z}_{{p_2}^{k_2}} \times \cdots \times \mathbf{Z}_{{p_m}^{k_m}}$$

where the p_i are prime and each $k_i \in \mathbf{Z}^+$. Let p be a prime number. Let n_k be the number of elements in G whose order divides p^k. Let a_k be the number of indices i such that $p_i = p$ and $k_i = k$. Let b_k be the number of indices i such that $p_i = p$ and $k_i \geq k$. Note that $a_k = b_k - b_{k+1}$. Using the fact that for $x_i \in \mathbf{Z}_{{p_i}^{k_i}}$ we have $\big|(x_1, x_2, \cdots, x_m)\big| = \mathrm{lcm}\big(|x_1|, |x_2|, \cdots, |x_m|\big)$, verify that

$$\begin{aligned} n_1 &= p^{b_1} \\ n_2 &= p^{a_1} p^{2b_2} \\ n_3 &= p^{a_1} p^{2a_2} p^{3b_3} \\ &\;\;\vdots \\ n_k &= p^{a_1} p^{2a_2} p^{3a_3} \cdots p^{(k-1)a_{k-1}} p^{kb_k} \end{aligned}$$

so we have

$$\frac{n_k}{n_{k-1}} = \frac{p^{(k-1)a_{k-1}} p^{kb_k}}{p^{(k-1)b_{k-1}}} = \frac{p^{(k-1)a_{k-1}} p^{kb_k}}{p^{(k-1)(a_{k-1}+b_k)}} = p^{b^k} \text{ , and so}$$

$$p^{a_k} = p^{b_k - b_{k+1}} = p^{b_k} \big/ p^{b_{k+1}} = \frac{n_k}{n_{k-1}} \Big/ \frac{n_{k+1}}{n_k} = \frac{{n_k}^2}{n_{k-1} n_{k+1}}.$$

This formula shows that the number of elements of each order in G determines the values of each prime p_i and each exponent k_i.

7.10 Corollary: *Let G and H be finite abelian groups. If G and H have the same number of elements of each order then $G \cong H$.*

7.11 Corollary: *Let $n = \prod {p_i}^{k_i}$ where the p_i are distinct primes and each $k_i \in \mathbf{Z}^+$. Then the number of distinct abelian groups of order n (up to isomorphism) is equal to $\prod P(k_i)$ where $P(k_i)$ is the number of partitions of k_i.*

Proof: The abelian groups of order p^k are the groups $\prod \mathbf{Z}_{p^{j_i}}$ where the j_i partition k.

.

Chapter 8. Definition and Examples of Rings and Subrings

8.1 Definition: A **ring** is a set R with two binary operations, addition denoted by $+$ and multiplication denoted by $\times$, by $\cdot$ or by concatenation, and an element $0 \in R$ such that
(1) $+$ is associative: $(a+b)+c = a+(b+c)$ for all $a,b,c \in R$,
(2) $+$ is commutative: $a+b = b+a$ for all $a,b,c \in R$,
(3) 0 is an additive identity: $a+0 = 0+a = a$ for all $a \in R$,
(4) every $a \in R$ has an additive inverse: there exists $b \in R$ such that $a+b = b+a = 0$,
(5) $\times$ is associative: $(ab)c = a(bc)$ for all $a,b,c \in R$, and
(6) $\times$ is distributive over $+$: $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all $a,b,c \in R$.

We say that R is **commutative** when $\times$ is commutative, that is $ab = ba$ for all $a,b \in R$. We say that R has an **identity** (or that R has a 1) when it has a multiplicative identity, that is when there is a non-zero element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. When R has a 1, for $a \in R$ we say that a is **invertible** (or that a is a **unit**) when there is an element $b \in R$ with $ab = 1 = ba$. A **division ring** is a ring R with identity such that every non-zero element of R is invertible. A **field** is a commutative division ring.

8.2 Theorem: (*Uniqueness of Identity and Inverse*) *Let R be a ring. Then*

(1) the additive identity 0 is unique in the sense that if $e \in R$ has the property that $a+e = a = e+a$ for all $a \in R$ then $e = 0$,
(2) the additive inverse of $a \in G$ is unique in the sense that for all $a,b,c \in G$ if we have $a+b = 0 = b+a$ and $a+c = 0 = c+a$ then $b = c$,
(3) if R has a 1, then it is unique in the sense that for all $u \in R$, if u has the property that $au = a = ua$ for all $a \in G$ then $u = 1$, and
(4) if R has a 1 and $a \in R$ has an inverse, then it is unique in the sense that for all $a \in G$ if there exist $b,c \in G$ such that $ab = ba = 1$ and $ac = ca = 1$ then $b = c$.

8.3 Notation: Let R be a ring. For $a \in R$ we denote the unique additive inverse of $a \in R$ by $-a$, and for $a,b \in R$ we write $b-a$ for $b+(-a)$. If R has a 1 and $a \in R$ has a multiplicative inverse, we say that a is a **unit** in R, and we denote its inverse by a^{-1}.

8.4 Theorem: (*Cancellation Under Addition*) *Let R be a ring. Then for all $a,b,c \in R$,*
(1) if $a+c = b+c$ then $a = c$,
(2) if $a+b = a$ then $b = 0$, and
(3) if $a+b = 0$ then $b = -a$.

8.5 Note: We do not, in general, have similar rules for cancellation under multiplication. In general, for a,b,c in a ring R, $ac = bc$ does not imply that $a = b$, $ac = a$ does not imply that $c = 1$, $ac = 1$ does not imply that $ca = 1$, and $ac = 0$ does not imply that $a = 0$ or $b = 0$. When $ac = 1$ we say that a is a **left inverse** for c and that c is a **right inverse** for a. When $ac = 0$ but $a \neq 0$ and $b \neq 0$, we say that a and b are **zero divisors**. A commutative ring with 1 which has no zero divisors is called an **integral domain**.

8.6 Theorem: (*Cancellation Under Multiplication*) *Let R be a ring. For all $a,b,c \in R$, if $ac = bc$, or if $ca = cb$, then either $a = b$ or $c = 0$ or c is a zero divisor.*

Proof: Suppose $ac = bc$. Then $ac - bc = 0$ so $(a-b)c = 0$. Either $(a-b) = 0$ so $a = b$, or $c = 0$ or $(a-b)$ and c are zero divisors. The case that $ca = cb$ is similar.

8.7 Theorem: (*Basic Properties of Rings*) *Let R be a ring. Then*
(1) $0 \cdot a = a \cdot 0 = 0$ *for all* $a \in R$,
(2) $(-a)b = -(ab) = a(-b)$ *for all* $a, b \in R$,
(3) $(-a)(-b) = ab$ *for all* $a, b \in R$,
(4) if R *has a 1 then* $(-1)a = -a$ *for all* $a \in R$.

Proof: Let $a \in R$. Then $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Thus $0 \cdot a = 0$ by additive cancellation. The proof that $a \cdot 0 = 0$ is similar, and the other proofs are left as an exercise.

8.8 Notation: Let R be a ring. For $k \in \mathbf{Z}^+$ we write $ka = a + a + \cdots + a$ with k terms in the sum, and we write $(-k)a = k(-a)$, and we write $a^k = a \cdot a \cdot \ldots \cdot a$ with k terms in the product. For $0 \in \mathbf{Z}$ we write $0a = 0$ and if R has a 1 we write $a^0 = 1$. If R has a 1 and $a \in R$ is a unit, we write $a^{-k} = (a^{-1})^k$. For all $k, l \in \mathbf{Z}$ and all $a \in R$ we have $(k+l)a = ka + la$, $(-k)a = -(ka) = k(-a)$, $-(-a) = a$, $-(a+b) = -a - b$, $(ka)(lb) = (kl)(ab)$. For $a \in R$ and $k, l \in \mathbf{Z}^+$ we have $a^{k+l} = a^k a^l$. When R has a 1 and a and b are units, then for $k, l \in \mathbf{Z}$ we have $a^{k+l} = a^k a^l$, $a^{-k} = (a^k)^{-1}$, $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.

8.9 Example: $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ and $\mathbf{Z}_n$ are all commutative rings with 1. Of these, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$, and also $\mathbf{Z}_p$ when p is prime, are fields.

8.10 Example: The ring of real **quaternions** is the set $\mathbf{H} = \mathbf{R}^4$ in which we write $1 = (1,0,0,0)$, $i = (0,1,0,0)$, $j = (0,0,1,0)$, $k = (0,0,0,1)$ and for $t \in \mathbf{R}$ we write $t = (t,0,0,0)$, $ti = it = (0,t,0,0)$, $tj = jt = (0,0,t,0)$ and $tk = kt = (0,0,0,t)$. We define addition as usual in $\mathbf{H} = \mathbf{R}^4$. and we define multiplication by requiring that $i^2 = j^2 = k^2 = -1$, that $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$, and that every real number commutes with i, j and k. It can be verified that $\mathbf{H}$ is a division ring with

$$(a + ib + jc + kd)^{-1} = \frac{a - ib - jc - kd}{a^2 + b^2 + c^2 + d^2}$$

for all $0 \neq a + ib + jc + kd \in \mathbf{H}$.

8.11 Example: For a set A and a ring R, the set

$$\text{Func}(A, R) = R^A = \big\{\text{fuctions } f : A \to R\big\}$$

is a ring under the operations given by $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in A$. If R is commutative then so is $\text{Func}(A, R)$. If R has identity 1 then the identity of $\text{Func}(A, R)$ is the constant function $1 : A \to R$ given by $1(x) = 1$ for all $x \in A$.

8.12 Example: For a group G, an **endomorphism** of G is a group homomorphism $\phi : G \to G$. If G is an additive abelian group then the set

$$\text{End}(G) = \big\{\text{endomorphisms } \phi : G \to G\big\}$$

is a ring under the operations given by $(\phi + \psi)(x) = \phi(x) + \psi(x)$ and $(\phi\psi)(x) = \phi\big(\psi(x)\big)$ for all $x \in G$. The ring $\text{End}(G)$ has an identity, namely the identity function $I : G \to G$ given by $I(x) = x$ for all $x \in G$.

8.13 Example: Let R be a ring with 1. Then the set

$$R^* = \big\{a \in R \big|\ a \text{ is a unit}\big\}$$

is a group under multiplication, called the **group of units** of R.

8.14 Example: For a ring R and a variable symbol x, a **formal power series** in x over R is a sequence $(a_0, a_1, a_2, \cdots)$ with each $a_i \in R$, and we write this sequence as

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots .$$

The elements a_i are called the **coefficients** of f and a_0 is called the **constant coefficient**. A power series of the form $f(x) = a$ with $a \in R$ is called a **constant series**. The set

$$R[[x]] = \big\{\text{formal power series in } x \text{ over } R\big\}$$

is a ring, which we call the **ring of formal power series** in x over R, with the following operations: for $f(x) = \sum\limits_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum\limits_{j=0}^{\infty} b_j x^j$ we have

$$(f+g)(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^i \text{ , and } (fg)(x) = \sum_{k=0}^{\infty} c_k x^k \text{ where } c_k = \sum_{i=0}^{k} a_i b_{k-i} .$$

If R is commutative then so is $R[[x]]$, and if R has identity 1 then the identity of $R[[x]]$ is the constant polynomial 1, that is the sequence $1 = (1, 0, 0, \cdots)$. A **polynomial** in x over R is a formal power series with only finitely non-zero coefficients. When we have $a_i = 0$ for all $i > n$ we also write $f(x) = \sum\limits_{i=0}^{n} a_i x^i$. When $a_n \neq 0$ and $a_i = 0$ for all $i > n$ we say that a_n is the **leading coefficient** of f and that the **degree** of f is $\deg(f) = n$. The set

$$R[x] = \big\{\text{polynomials in } x \text{ over } R\big\}$$

is a ring, which we call the **ring of polynomials** in x over R, using the same operations as in $R[[x]]$.

8.15 Example: For a ring R and variable symbols $x_1, \cdots, x_n$, a **formal power series** in $x_1, \cdots, x_n$ over R is a function $a : \mathbf{N}^n \to R$, and we write this function as

$$f(x_1, \cdots, x_n) = \sum_{(i_1, \cdots, i_n) \in \mathbf{N}^n} a_{i_1, \cdots, i_n} {x_1}^{i_1} \cdots {x_n}^{i_n} \text{ where } a_{i_1, \cdots, i_n} = a(i_1, \cdots, i_n) .$$

The elements $a_{i_1, \cdots, i_n} \in R$ are called the **coefficients** of the power series. The set

$$R[[x_1, \cdots, x_n]] = \big\{\text{formal power series in } x_1, \cdots, x_n \text{ over } R\big\}$$

is a ring, called the **ring of formal power series** in $x_1, \cdots, x_n$ over R, under the following operations: for $f(x) = \sum a_{i_1, \cdots, i_n} {x_1}^{i_1} \cdots {x_n}^{i_n}$ and $g(x) = \sum b_{j_1, \cdots, j_n} {x_1}^{j_1} \cdots {x_n}^{j_n}$ we define

$$(f+g)(x) = \sum (a_{k_1, \cdots, k_n} + b_{k_1, \cdots, k_n}) {x_1}^{k_1} \cdots {x_n}^{k_n}$$
$$(fg)(x) = \sum c_{k_1, \cdots, k_n} {x_1}^{k_1} \cdots {x_n}^{k_n}$$

where $c_{k_1, \cdots, k_n}$ is the sum of all terms $a_{i_1, \cdots, i_n} b_{j_1, \cdots, j_n}$ for which $i_\alpha + j_\alpha = k_\alpha$ for all $\alpha = 1, \cdots, n$. A **polynomial** in $x_1, \cdots, x_n$ over R is a formal power series with only finitely many non-zero coefficients, and the set

$$R[x_1, x_2, \cdots, x_n] = \big\{\text{polynomials in } x_1, \cdots, x_n \text{ over } R\big\}$$

is a ring using the same operations as in $R[[x_1, \cdots, x_n]]$.

8.16 Example: For a ring R, the set

$$M_n(R) = \{n \times n \text{ matrices with entries in } R\}$$

is a ring under matrix addition and matrix multiplication, which we call the **ring of** $n \times n$ **matrices over** R. If R has identity 1 then the identity of $M_n(R)$ is the $n \times n$ identity matrix I.

8.17 Example: If R and S are rings then the cartesian product

$$R \times S = \{(a, b) \big| a \in R, b \in S\}$$

is a ring, called the **product ring** of R and S, with operations

$$(a, b) + (c, d) = (a + c, b + d) \text{ and } (a, b)(c, d) = (ac, bd)\,.$$

More generally, if $R_1, \cdots, R_n$ are rings then so is the product

$$\prod_{i=1}^{n} R_i = R_1 \times \cdots \times R_n = \{(a_1, \cdots, a_n) \big| \text{each } a_i \in R_i\}\,,$$

which we call the **product ring** of $R_1, \cdots, R_n$, under the operations

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = \big(a_1 + b_1, \cdots, a_n + b_n\big) \text{ , and}$$
$$(a_1, \cdots, a_n)(b_1, \cdots, b_n) = \big(a_1, b_1, \cdots, a_n b_n\big)\,.$$

More generally still, if A is any set and R_α is a ring for each $\alpha \in A$, then the product

$$\prod_{\alpha \in A} R_\alpha = \{f : A \to \bigcup_{\alpha \in A} R_\alpha \big| f(\alpha) \in R_\alpha \text{ for all } \alpha \in A\}$$

is a ring, called the **product ring** of the rings $R_\alpha, \alpha \in A$, under the operations

$$(f + g)(\alpha) = f(\alpha) + g(\alpha) \text{ and } (fg)(\alpha) = f(\alpha)g(\alpha).$$

8.18 Theorem: *Let R be a finite ring. Then R is a field if and only if R is an integral domain.*

Proof: Suppose that R is a field. Let $a, b \in R$. Suppose that $ab = 0$ and $a \neq 0$. Then $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Thus R has no zero divisors.

Conversely, suppose that R is an integral domain. We must show that every non-zero element in R is a unit. Let $0 \neq a \in R$. Consider the left multiplication map $L_a : R \to R$ given by $L_a(x) = ax$. For $x, y \in R$ we have $L_a(x) = L_a(y) \Longrightarrow ax = ay \Longrightarrow x = y$ by cancellation, since $a \neq 0$ and a is not a zero divisor. Thus L_a is injective. Since R is finite, this implies that L_a is bijective. In particular, we can choose $b \in R$ so that $L_a(b) = 1$, that is $ab = 1$. Similarly, right multiplication R_a is bijective, and so we can choose $c \in R$ so that $ca = 1$. Then we have $c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b$, and so a is a unit with $a^{-1} = b = c$.

8.19 Definition: Let R be a ring with 1. We define the **characteristic** of R, written as $\mathrm{char}(R)$, to be the smallest $n \in \mathbf{Z}^+$ such that $n \cdot 1 = 0$ if such an n exists, and if no such n exists then the characteristic of R is 0. Note that when $n \cdot 1 = 0$ we have $n \cdot a = 0$ for all $a \in R$ because $n\,a = a + a + \cdots + a = (1 + 1 + \cdots 1)a = (n \cdot 1)\,a$.

8.20 Theorem: L*et* R *be a ring with 1 with no zero divisors. Then either* $\text{char}(R) = 0$ *or* $\text{char}(R)$ *is prime.*

Proof: Suppose $\text{char}(R) = n \in \mathbf{Z}^+$. Suppose, for a contradiction, that n is composite, say $n = kl$ with $1 < k, l < n$. Then $0 = n \cdot 1 = (kl) \cdot 1 = (k \cdot 1)(l \cdot 1)$. Since R has no zero divisors, either $k \cdot 1 = 0$ or $l \cdot 1 = 0$. This contradicts the definition of $n = \text{char}(R)$.

8.21 Definition: A **subring** of a ring R is a subset $S \subseteq R$ which is a ring using the same operations used in R. Similarly, a **subfield** of a field F is a subset $K \subseteq F$ which is also a field using the same operations used in F.

8.22 Theorem: I*f* S *be a subset of a ring* R*, then* S *is a subring of* R *if and only if*
(1) $0 \in S$,
(2) S *is closed under addition, that is* $a + b \in S$ *for all* $a, b \in S$,
(3) S *is closed under multiplication, that is* $ab \in S$ *for all* $a, b \in S$*, and*
(4) S *is closed under additive inverse, that is* $-a \in S$ *for all* $a \in S$.

Similarly, if K *is a subset of a field* F *then* K *is a subfield of* F *if and only if*
(1) $0 \in K$ *and* $1 \in K$,
(2) K *is closed under addition, that is* $a + b \in K$ *for all* $a, b \in K$,
(3) K *is closed under multiplication, that is* $ab \in K$ *for all* $a, b \in K$,
(4) K *is closed under additive inverse, that is* $-a \in S$ *for all* $a \in K$*, and*
(5) K *s closed under multiplicative inverse, that is* $a^{-1} \in K$ *for all* $0 \neq a \in F$.

8.23 Example: $\mathbf{Z}$ is a subring of $\mathbf{Q}$, $\mathbf{Q}$ is a subring of $\mathbf{R}$, $\mathbf{R}$ is a subring of $\mathbf{C}$, and $\mathbf{C}$ is a subring of $\mathbf{H}$. Also, $\mathbf{Q}$ is a subfield of $\mathbf{R}$ which is a subfield of $\mathbf{C}$.

8.24 Example: In $\mathbf{Z}$, the subgroups are of the form $\langle n \rangle = \{kn \big| k \in \mathbf{Z}\}$ where $0 \leq n \in \mathbf{Z}$. Each of these subgroups is also a subring of $\mathbf{Z}$. In $\mathbf{Z}_n$, the subgroups are of the form $\langle d \rangle = \{kd | k \in \mathbf{Z}_{n/d}\}$ where $d | n$, and each of these subgroups is also a subring.

8.25 Example: In $\mathbf{Z}_{12}$ we have the subring $\langle 3 \rangle = \{0, 3, 6, 9\}$. Notice that $9 \cdot 0 = 0$, $9 \cdot 3 = 3$, $9 \cdot 6 = 6$ and $9 \cdot 9 = 9$, so 9 is the identity element in the group $\langle 3 \rangle$. This example shows that the identity element in a subring of R does not need to be equal to the identity element of R.

8.26 Example: Define

$$\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} \big| a, b \in \mathbf{Z}\} \text{ , and}$$
$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \big| a, b \in \mathbf{Q}\} .$$

Then $\mathbf{Z}[\sqrt{2}]$ is a subring of $\mathbf{R}$ and $\mathbf{Q}[\sqrt{2}]$ is a subring of $\mathbf{R}$ because

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} .$$

In fact $\mathbf{Q}[\sqrt{2}]$ is a subfield of $\mathbf{R}$ because for $a, b \in \mathbf{Q}$, if $a + b\sqrt{2} \neq 0$ then $a^2 \neq 2b^2$ and

$$(a + b\sqrt{2}) \left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \right) = 1 .$$

8.27 Example: More generally, if R is a subring of S and $A \subseteq S$, then we write $R[A]$ for the smallest subring of S which contains R and A, or equivalently the intersection of all subrings of S which contain $R \cup A$. Some particular cases of this include the subrings

$$\begin{aligned} \mathbf{Z}[i] &= \big\{ a + bi \,\big|\, a, b \in \mathbf{Z} \big\} \subseteq \mathbf{C} \\ \mathbf{Q}[\alpha] &= \big\{ a + b\alpha + c\alpha^2 \,\big|\, a, b, c \in \mathbf{Q} \big\} \subseteq \mathbf{C} \text{ , where } \alpha = e^{i\,2\pi/3} \\ \mathbf{Q}[\sqrt{2}, \sqrt{3}] &= \big\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \,\big|\, a, b, c, d \in \mathbf{Q} \big\} \subseteq \mathbf{R}. \end{aligned}$$

As an exercise, check that these are all rings and that $\mathbf{Q}[\alpha]$ and $\mathbf{Q}[\sqrt{2}, \sqrt{3}]$ are fields.

8.28 Example: We sometimes use notation, similar to the notation used in the above example, for some other rings. For example, we write

$$\mathbf{Z}_n[i] = \big\{ a + bi \,\big|\, a, b \in \mathbf{Z}_n \big\} .$$

This is a ring under the operations given by $(a + bi) + (c + di) = (a + c) + (b + d)i$ and $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

8.29 Example: For an interval $A \subseteq \mathbf{R}$, let $\mathcal{C}^0(A, \mathbf{R})$ denote the set of continuous functions $f : A \to \mathbf{R}$, for $k \in \mathbf{Z}^+$ let $\mathcal{C}^k(A, \mathbf{R})$ denote the set of functions $f : A \to \mathbf{R}$ such that the k^{th} derivative $f^{(k)}$ exists and is continuous in A, and let $\mathcal{C}^\infty(A, \mathbf{R})$ denote the set of infinitely differentiable functions $f : A \to \mathbf{R}$. Then $\mathcal{C}^\infty(A, \mathbf{R})$ is a subring of $\mathcal{C}^k(A, \mathbf{R})$ which is a subring of $\mathcal{C}^0(A, \mathbf{R})$ which, in turn, is a subring of $\text{Func}(A, \mathbf{R})$.

8.30 Example: For a ring R, the polynomial ring $R[x]$ is a subring of the formal power series ring $R[[x]]$. More generally, $R[x_1, \cdots, x_n]$ is a subring of $R[[x_1, \cdots, x_n]]$. If S is a subring of R then $S[x]$ is a subring of $R[x]$ and $S[[x]]$ is a subring of $R[[x]]$, and more generally, $S[x_1, \cdots, x_n]$ is a subring of $R[x_1, \cdots, x_n]$ and $S[[x_1, \cdots, x_n]]$ is a subring of $R[[x_1, \cdots, x_n]]$. We can regard R as a subring of $R[x]$ by identifying an element $a \in R$ with the corresponding constant polynomial in $R[x]$. Similarly, we can regard $R[x_1, \cdots, x_n]$ as a subring of $R[x_1, \cdots, x_n, x_{n+1}]$ and $R[[x_1, \cdots, x_n]]$ as a subring of $R[[x_1, \cdots, x_n, x_{n+1}]]$.

8.31 Example: Although we can regard the polynomial ring $\mathbf{R}[x]$ as a subring of the ring of functions $\text{Func}(\mathbf{R}, \mathbf{R})$ (since we can regard a polynomial as a kind of function), in general given a ring R we cannot regard $R[x]$ as a subring of $\text{Func}(R, R)$. For example, if R is finite, say with $|R| = n$, then $\big|\text{Func}(R, R)\big| = n^n$ but $\big|R[x]\big| = \infty$ (or more precisely $\big|R[x]\big| = \aleph_0$).

8.32 Example: For a ring R, the set $T_n(R)$ of upper-triangular matrices with entries in R is a subring of $M_n(R)$. If S is a subring of R then $M_n(S)$ is a subring of $M_n(R)$.

8.33 Definition: For a ring R, we define the **centre** of R to be the ring

$$Z(R) = \big\{ a \in R \big| ax = xa \text{ for all } x \in R \big\}.$$

As an exercise, verify that $Z(R)$ is in fact a subring of R.

Chapter 9. Ring Homomorphisms, Ideals and Quotient Rings

9.1 Definition: Let R and S be rings. A **ring homomorphism** from R to S is a map $\phi : R \to S$ such that

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and}$$
$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in R$. The **kernel** of ϕ is the set

$$\text{Ker}(\phi) = \phi^{-1}(0) = \big\{a \in R \big| \phi(a) = 0\big\}$$

and the **image** (or **range**) of ϕ is the set

$$\text{Image}(\phi) = \phi(R) = \big\{\phi(a) \big| a \in R\big\}\,.$$

A ring **isomorphism** from R to S is a bijective ring homomorphism from R to S. For two rings R and S, we say that R and S are **isomorphic**, and we write $R \cong S$, when there exists an isomorphism $\phi : R \to S$.

9.2 Theorem: *Let $\phi : R \to S$ be a ring homomorphism. Then*

(1) $\phi(0) = 0$,
(2) for $a \in R$ we have $\phi(ka) = k\phi(a)$ for all $k \in \mathbf{Z}$,
(3) if R has a 1 and ϕ is surjective, then S has a 1 and $\phi(1) = 1$,
(4) for $a \in R$ we have $\phi(a^k) = \phi(a)^k$ for all $k \in \mathbf{Z}^+$, and
(5) if R has a 1, ϕ is surjective, and $a \in R$ is a unit, then $\phi(a^k) = \phi(a)^k$ for all $k \in \mathbf{Z}$.

9.3 Theorem: *Let $\phi : R \to S$ and $\psi : S \to T$ be ring homomorphisms. Then*

(1) the identity map $I : R \to R$ is a ring homomorphism,
(2) the composite $\psi \circ \phi : R \to T$ is a homomorphism, and
(3) if ϕ is bijective then the inverse $\phi^{-1} : S \to R$ is a homomorphism.

9.4 Corollary: I*somorphism is an equivalence relation on the class of rings.*

9.5 Theorem: *Let $\phi : R \to S$ be a ring homomorphism. Then*

(1) If K is a subgroup of R then $\phi(K)$ is a subgroup of S. In particular, Image(ϕ) is a subgroup of S.
(2) if L is a subgroup of S then $\phi^{-1}(L)$ is a subgroup of R. In particular, Ker(ϕ) is a subgroup of R.

9.6 Theorem: *Let $\phi : R \to S$ be a ring homomorphism. Then*

(1) ϕ is injective if and only if Ker(ϕ) $= \{0\}$, and
(2) ϕ is surjective if and only if Image(ϕ) $= S$.

9.7 Example: For rings R and S, the **zero function** $0 : R \to S$, given by $0(x) = 0$ for all $x \in R$, is a ring homomorphism. For a ring R, the **identity function** $I : R \to R$, given by $I(x) = x$ for all $x \in R$, is a ring homomorphism.

9.8 Example: Let R be a ring. For $a \in R$, define $\phi_a : \mathbf{Z} \to R$ by $\phi_a(k) = ka$. Show that the ring homomorphisms $\phi : \mathbf{Z} \to R$ are the maps $\phi = \phi_a$ with $a \in R$ such that $a^2 = a$.

Solution: For $a \in R$, let $\phi_a : \mathbf{Z} \to R$ be the map given by $\phi_a(k) = ka$. Note that for any ring homomorphism $\phi : \mathbf{Z} \to R$, if we let $a = \phi(1)$ then for all $k \in \mathbf{Z}$ we have $\phi(k) = \phi(k\cdot 1) = k\cdot\phi(1) = ka = \phi_a(k)$. Thus every ring homomorphism $\phi : \mathbf{Z} \to R$ is of the form $\phi = \phi_a$ for some $a \in R$. Also note that in order for ϕ_a to be a ring homomorphism, we must have $a^2 = \phi(1)^2 = \phi(1^2) = \phi(1) = a$. Finally, note that given $a \in R$ with $a^2 = a$, the map ϕ_a is a ring homomorphism because $\phi_a(k+l) = (k+l)a = ka + la = \phi_a(k) + \phi_l(a)$ and $\phi_a(kl) = (kl)a = (kl)a^2 = (ka)(la) = \phi_a(k)\phi_l(a)$. Thus the ring homomorphisms from $\mathbf{Z}$ to R are precisely the maps ϕ_a where $a \in R$ with $a^2 = a$.

9.9 Example: Let R be a ring. For $a, b \in R$, define the map $\phi_{a,b} : \mathbf{Z} \times \mathbf{Z} \to R$ by $\phi_{a,b}(k, l) = (ka)(lb)$. As an exercise, show that the ring homomorphisms $\phi : \mathbf{Z} \times \mathbf{Z} \to R$ are the maps $\phi = \phi_{a,b}$ with $a, b \in R$ such that $a^2 = a$, $b^2 = b$ and $ab = ba = 0$.

9.10 Definition: An element a in a ring R is called **idempotent** when $a^2 = a$.

9.11 Example: The complex conjugation map $\phi : \mathbf{C} \to \mathbf{C}$ given by $\phi(z) = \overline{z}$ is a ring homomorphism since $\overline{z + w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\,\overline{w}$, but the norm map $\psi(z) = ||z||$ is not a ring homomorphism because, in general, we do not have $||z + w|| = ||z|| + ||w||$.

9.12 Definition: Let R be a ring. For $a \in R$, the map $\phi_a : R[x] \to R$ given by $\phi_a\big(f(x)\big) = f(a)$, that is by

$$\phi_a\Big(\sum_{i=0}^{n} c_i x^i\Big) = \sum_{i=0}^{n} c_i a^i,$$

is called the **evaluation map** at a. If $a \in Z(R)$ then ϕ_a is a homomorphism because for $f = \sum b_i x^i$ and $g = \sum c_i x^i$ we have

$$\phi_a(f + g) = \phi_a\big(\sum_i (b_i + c_i)x^i\big) = \sum_i (b_i + c_i)a^i = \sum_i b_i a^i + \sum_i c_i x^i = \phi_a(f) + \phi_a(g)$$
$$\phi_a(fg) = \phi_a\big(\sum_{i,j} b_i c_j x^{i+j}\big) = \sum_{i,j} b_i c_j a^{i+j} = \sum_{i,j} b_i a^i c_j a^j = \sum_i b_i x^i \sum_j c_j a^j = \phi_a(f)\phi_a(g).$$

The **evaluation map** $\phi : R[x] \to \text{Func}(R, R)$ is then given by $\phi(f)(a) = \phi_a(f) = f(a)$, in other words ϕ sends the polynomial $f(x) = \sum c_i x^i$ to the function $f(x) = \sum c_i x^i$. If R is commutative, then the above calculation shows that this map ϕ is a homomorphism. If R is not commutative, then the multiplication operations in $R[x]$ and in $\text{Func}(R, R)$ are different and the evaluation map is not a homomorphism (in fact we are usually only interested in the polynomial ring $R[x]$ in the case that R is commutative).

9.13 Example: Show that $\mathbf{R} \not\cong \mathbf{C}$ (as rings).

Solution: If $\phi : \mathbf{R} \to \mathbf{C}$ was a ring isomorphism, then the restriction of ϕ to $\mathbf{R}^*$ would be a group isomorphism $\phi : \mathbf{R}^* \to \mathbf{C}^*$. But we know that the groups $\mathbf{R}^*$ and $\mathbf{C}^*$ are not isomorphic.

9.14 Example: Show that $2\mathbf{Z} \not\cong 3\mathbf{Z}$ (as rings).

Solution: In $2\mathbf{Z}$ we have $2 \cdot 2 = 4 = 2 + 2$, but there is no element $0 \neq a \in 3\mathbf{Z}$ with $a \cdot a = a + a$.

9.15 Theorem: (*Ideals and Quotient Rings*) *Let S be a subring of a ring R. Note that S is a subgroup of R under addition. Let R/S be the quotient group $R/S = \{a+S \big| a \in \mathbf{R}\}$ with addition operation given by $(a+S)+(b+S) = (a+b)+S$. We can define a multiplication operation on R/S by*

$$(a+S)(b+S) = ab + S$$

if and only if S has the property that for all $r \in R$ and $s \in S$ we have

$$rs \in S \text{ and } sr \in S.$$

In this case R/S is a ring under the above addition and multiplication operations. If R has identity 1, then R/S has identity $1+S$.

Proof: Suppose the formula $(a+S)(b+S) = ab+S$ gives a well-defined operation on R/S. Then for all $a_1, a_2, b_1, b_2 \in R$, if $a_1+S = a_2+S$ and $b_1+S = b_2+S$ then $a_1b_1+S = a_2b_2+S$. Equivalently, for all $a_1, b_1, a_2, b_2 \in R$, if $a_1 - a_2 \in S$ and $b_1 - b_2 \in S$ then $a_1a_2 - b_1b_2 \in S$. Let $r \in R$ and $s \in S$. Taking $a_1 = a_2 = r$, $b_1 = s$ and $b_2 = 0$, we have $a_1 - a_2 = 0 \in S$ and $b_1 - b_2 = s \in S$ and so $rs = a_1b_1 - a_2b_2 \in S$. Similarly, taking $a_1 = s$, $a_2 = 0$ and $b_1 = b_2 = r$ we see that $sr \in S$.

Conversely, suppose that for all $r \in R$ and $s \in S$ we have $rs \in S$ and $sr \in S$. Let $a_1, a_2, b_1, b_2 \in R$ with $a_1 - a_2 \in S$ and $b_1 - b_2 \in S$. Say $a_1 - a_2 = s \in S$ and $b_1 - b_2 = t \in S$. Then $a_1b_1 - a_2b_2 = a_1b_1 - (a_1-s)(b_1-t) = a_1b_1 - (a_1b_1 - a_1t - s\,b_1 + st) = a_1t + s\,b_1 + st \in S$. Thus the formula $(a+S)(b+S) = ab+S$ gives a well-defined operation on R/S.

Now we suppose that S has the required property so that $(a+S)(b+S) = ab+S$ does give a well-defined multiplication operation. This multiplication is associative because

$$\begin{aligned}\big((a+S)(b+S)\big)(c+S) &= (ab+S)(c+S) = (ab)c + S = a(bc)+S \\ &= (ab+S)(c+S) = (a+S)\big((b+S)(c+S)\big)\end{aligned}$$

and it is distributive over the addition operation on R/S because

$$\begin{aligned}(a+S)\big((b+S)+(c+S)\big) &= (a+S)\big((b+c)+S\big) = a(b+c)+S = ab+ac+S \\ &= (ab+S)+(ac+S) = (a+S)(b+S)+(a+S)(c+S)\end{aligned}$$

and similarly $\big((a+S)+(b+S)\big)(c+S) = (a+S)(c+S)+(b+S)(c+S)$. Thus R/S is a ring under these two operations.

9.16 Definition: Let R be a ring. An **ideal** in R is a subring $A \subseteq R$ with the property that for all $r \in R$ and $a \in A$ we have $ra \in A$ and $ar \in A$. When A is an ideal in R, the ring R/A, equipped with the operations of the above theorem, is called the **quotient ring** of R by A. It is easy to check that the zero element in R/A is $0+A$, the additive inverse of $a+A$ in R/A is $-(a+A) = -a+A$, if R has identity 1 then R/A has identity $1+A$, and if $a \in R$ is a unit then $a+A$ is a unit in R/A with $(a+A)^{-1} = a^{-1}+A$.

9.17 Example: In the cyclic group $\mathbf{Z}$, the subgroups are the groups $\langle n\rangle = n\mathbf{Z}$ with $n \geq 0$. Each of these subgroups is also an ideal in the ring $\mathbf{Z}$. For $n \in \mathbf{Z}^+$, the ring $\mathbf{Z}_n$ is the quotient ring $\mathbf{Z}_n = \mathbf{Z}/\langle n\rangle = \mathbf{Z}/n\mathbf{Z}$.

9.18 Example: In the group $\mathbf{Z}_n$ the subgroups are the groups $\langle d\rangle$ where $d \big| n$. Each of the subgroups is also an ideal in the ring $\mathbf{Z}_n$.

9.19 Example: In the group $\mathbf{Q}$, we have the subgroup $\langle 2\rangle = \{\cdots, -2, 0, 2, 4, \cdots\} = 2\mathbf{Z}$. This subgroup is also a subring of $\mathbf{Q}$ because it is closed under multiplication. But it is not an ideal in $\mathbf{Q}$ because it is not closed under multiplication by elements in $\mathbf{Q}$, for example $2 \in \langle 2\rangle$ and $\frac{1}{2} \in \mathbf{Q}$, but $1 = 2 \cdot \frac{1}{2} \notin \langle 2\rangle$.

9.20 Definition: Let R be a ring and let $U \subseteq R$. The **ideal in R generated by U**, denoted by $\langle U\rangle$, is the smallest ideal in R which contains U, or equivalently, the intersection of all ideals in R which contain U. The elements in U are called **generators** of $\langle U\rangle$. When U is finite we often omit the set brackets, so for $U = \{u_1, u_2, \cdots, u_n\}$ we write $\langle U\rangle = \langle u_1, u_2, \cdots, u_n\rangle$. An ideal of the form $\langle u_1, u_2, \cdots, u_n\rangle$ for some $u_i \in R$ is said to be **finitely generated**. An ideal of the form $\langle u\rangle$ for some $u \in R$ is called a **principal ideal**.

9.21 Theorem: *Let R be a ring and let U be a non-empty subset of R.*

(1) If R has a 1 then $\langle U\rangle = \left\{ \sum_{i=1}^{n} r_i u_i s_i \,\middle|\, n \in \mathbf{Z}^+, u_i \in U, r_i, s_i \in R \right\}$.

(2) If R is commutative with 1 then $\langle U\rangle = \left\{ \sum_{i=1}^{n} u_i r_i \,\middle|\, n \in \mathbf{Z}^+, u_i \in U, r_i \in R \right\}$. *In particular, for $a \in R$ we have* $\langle a\rangle = \left\{ ar \,\middle|\, r \in R \right\}$.

9.22 Note: In a field F, the only ideals are $\{0\}$ and F. Indeed let A be an ideal in F with $A \neq \{0\}$. Choose $0 \neq a \in A$. Since $a \in A$ and $a^{-1} \in F$, we must have $1 = a\,a^{-1} \in A$. Given any element $x \in F$, since $1 \in A$ and $x \in F$ we must have $x = x \cdot 1 \in A$. Thus $A = F$.

9.23 Definition: Let A and B be ideals in a ring R. The **intersection**, **sum** and the **product** of A and B are the sets

$$\begin{aligned} A \cap B &= \left\{ a \in R \,\middle|\, a \in A \text{ and } a \in B \right\}, \\ A + B &= \left\{ a + b \,\middle|\, a \in A, b \in B \right\} \text{ , and} \\ AB &= \left\{ \sum_{i=1}^{n} a_i b_i \,\middle|\, n \in \mathbf{Z}^+, a_i \in A, b_i \in B \right\}. \end{aligned}$$

As an exercise, show that $A \cap B$, $A + B$ and AB are all ideals in R.

9.24 Example: In $\mathbf{Z}$, for $k, l \in \mathbf{Z}^+$ verify that

$$\begin{aligned} \langle k\rangle \cap \langle l\rangle &= \langle m\rangle \text{ where } m = \text{lcm}(k, l) \\ \langle k\rangle + \langle l\rangle &= \langle d\rangle \text{ where } d = \gcd(k, l), \text{ and} \\ \langle k\rangle\langle l\rangle &= \langle kl\rangle. \end{aligned}$$

9.25 Theorem: (*The First Isomorphism Theorem*) *Let $\phi : R \to S$ be a homomorphism of rings. Let $K = \text{Ker}((\phi)$. Then K is an ideal in R and we have $R/K \cong \phi(R)$. Indeed the map $\Phi : R/K \to \phi(R)$ given by $\Phi(a + K) = \phi(a)$ is a ring isomorphism.*

9.26 Theorem: (*The Second Isomorphism Theorem*) *Let A and B be ideals in a ring R. Then A is an ideal in $A + B$, $A \cap B$ is an ideal in B, and*

$$(A + B)/A \cong B/(A \cap B).$$

9.27 Theorem: (*The Third Isomorphism Theorem*) *Let A and B be ideals in a ring R with $A \subseteq B \subseteq R$. Then B/A is an ideal in R/A and*

$$(R/A)\big/(B/A) \cong R/B.$$

9.28 Example: Let $d, n \in \mathbf{Z}^+$ with $d \big| n$. Then the map $\phi : \mathbf{Z}_n \to \mathbf{Z}_d$ given by $\phi(k) = k$ is a ring homomorphism with $\text{Ker}(\phi) = \langle d \rangle$. By the First Isomorphism Theorem, we have $\mathbf{Z}_n / \langle d \rangle \cong \mathbf{Z}_d$.

9.29 Example: Define a map $\phi : \mathbf{Q}[x] \to \mathbf{Q}[\sqrt{2}]$ by $\phi(f) = f(\sqrt{2})$. Then ϕ is a homomorphism because $\phi(f+g) = (f+g)(\sqrt{2}) = f(\sqrt{2}) + g(\sqrt{2}) = \phi(f) + \phi(g)$ and $\phi(fg) = (fg)(\sqrt{2}) = f(\sqrt{2})g(\sqrt{2}) = \phi(f)\phi(g)$. Also note that ϕ is surjective because $\phi(a + bx) = a + b\sqrt{2}$ for $a, b \in \mathbf{Q}$. Finally note that for $f \in \mathbf{Q}[x]$ we have

$$\begin{aligned} f(x) \in \text{Ker}(\phi) &\iff f(\sqrt{2}) = 0 \in \mathbf{R} \iff f(\sqrt{2}) = f(-\sqrt{2}) = 0 \in \mathbf{R} \\ &\iff (x^2 - 2) \big| f(x) \iff f(x) \in \langle x^2 - 2 \rangle, \end{aligned}$$

where we used the fact that for $f(x) = \sum c_i x^i \in \mathbf{Q}[x]$ we have

$$f(\pm\sqrt{2}) = \left(\sum c_{2k} 2^k \right) \pm \left(\sum c_{2k+1} 2^k \right) \sqrt{2}$$

so that $f(\sqrt{2}) = 0 \iff f(-\sqrt{2}) = 0 \iff \sum c_{2k} 2^k = 0 = \sum c_{2k+1} 2^k$. By the First Isomorphism Theorem, we have $\mathbf{Q}[x] / \langle x^2 - 2 \rangle \cong \mathbf{Q}[\sqrt{2}]$.

9.30 Example: Define $\phi : \mathbf{R}[x] \to \mathbf{C}$ by $\phi(f) = f(i)$. Then ϕ is a homomorphism since $\phi(f+g) = (f+g)(i) = f(i) + g(i) = \phi(f) + \phi(g)$ and $\phi(fg) = (fg)(i) = f(i)g(i) = \phi(f)\phi(g)$. The map ϕ is surjective because $\phi(a + bx) = a + bi$ for $a, b \in \mathbf{R}$. Also, for $f(x) \in \mathbf{R}[x]$,

$$f(x) \in \text{Ker}(\phi) \iff f(i) = 0 \in \mathbf{C} \iff (x^2+1) \big| f(x) \in \mathbf{R}[x] \iff f(x) \in \langle x^2+1 \rangle \subseteq \mathbf{R}[x].$$

Thus by the First Isomorphism Theorem, we have $\mathbf{R}[x] / \langle x^2 + 1 \rangle \cong \mathbf{C}$.

9.31 Example: Define $\phi : \mathbf{Z}[i] \to \mathbf{Z}_5$ by $\phi(a + bi) = a + 2b$. The map ϕ is a ring homomorphism because

$$\begin{aligned} \phi\big((a+bi) + (c+di)\big) &= \phi\big((a+c) + (b+d)i\big) = (a+c) + 2(b+d) \\ &= (a+2b) + (c+2d) = \phi(a+bi) + \phi(c+di) \text{ , and} \\ \phi\big((a+bi)(c+di)\big) &= \phi\big((ac-bd) + (ad+bc)i\big) = (ac-bd) + 2(ad+bc) \\ &= ac + 2ad + 2bc + 4bd = (a+2b)(c+2d) = \phi(a+bi)\phi(c+di). \end{aligned}$$

Also note that ϕ is surjective because $\phi(a + 0i) = a$. Finally, note that

$$a + bi \in \text{Ker}(\phi) \iff a + 2b = 0 \in \mathbf{Z}_5 \iff b = 2a \in \mathbf{Z}_5 \iff a + ib \in \langle 2 - i \rangle,$$

indeed if $b = 2a$ then we have $a + bi = a + 2a\,i = (2-i)(ai) \in \langle 2 - i \rangle$ and conversely, if $a + bi \in \langle 2 - i \rangle$, say $a + bi = (2-i)(x+yi) = (2x+y) + (2y-x)i$, then we have $a = 2x + y$ and $b = 2y - x$ so that $2a = 2(2x+y) = 4x + 2y = 2y - x = b \in \mathbf{Z}_5$. By the First Isomorphism Theorem, we have $\mathbf{Z}[i] / \langle 2 - i \rangle \cong \mathbf{Z}_5$.

9.32 Definition: Let R be a commutative ring. Consider the evaluation homomorphism $\phi : R[x] \to \text{Func}(R,R)$ given by $\phi(f) = f$, that is the map which sends the polynomial $f(x)$ to the function $f(x)$. A polynomial $f \in R[x]$ is equal to zero when all of its coefficients are equal to zero. A function $f \in \text{Func}(R,R)$ is equal to zero when we have $f(a) = 0$ for all $a \in R$. The kernel of the evaluation homomorphism is

$$\text{Ker}(\phi) = \big\{ f \in R[x] \,\big|\, f(a) = 0 \text{ for all } a \in R \big\}.$$

The image $\phi\big(R[x]\big) \subseteq \text{Func}(R,R)$ is called the **ring of polynomial functions** on R. By the First Isomorphism Theorem, it is isomorphic to the quotient ring $R[x]\big/\text{Ker}(\phi)$.

9.33 Example: If R is an infinite field, then $\text{Ker}(\phi) = 0$ since for $f(x) \in R[x]$, if $f(a) = 0$ for all $a \in R$ then $f(x)$ has infinitely many roots, and so $f(x) = 0$ as a polynomial (a non-zero polynomial of degree $n \geq 0$ over a field has at most n roots). In this case, ϕ is injective so the polynomial ring $R[x]$ is isomorphic to the ring of polynomial functions $\phi\big(R[x]\big) \subseteq \text{Func}(R,R)$, and we often identify $R[x]$ with $\phi\big(R[x]\big)$.

If R is a finite field, the situation is quite different. In this case $R[x]$ is infinite but $\text{Func}(R,R)$ is finite, so $R[x]$ is certainly not isomorphic to a subring of $\text{Func}(R,R)$. Let us consider the case that $R = \mathbf{Z}_p$ where p is prime. By Fermat's Little Theorem, we know that $a^p = a$ for all $a \in \mathbf{Z}_p$, and so every $a \in \mathbf{Z}^p$ is a root of the polynomial $p(x) = x^p - x$. Since there are exactly p elements in $\mathbf{Z}_p$, it follows that $p(x)$ factors as

$$p(x) = x^p - x = (x-0)(x-1)(x-2)\cdots(x-(p-1)).$$

For a polynomial $f(x) \in \mathbf{Z}_p[x]$ we have

$$\begin{aligned} f(x) \in \text{Ker}(\phi) &\iff f(a) = 0 \text{ for all } a \in \mathbf{Z}_p \iff (x-a)\big|f(x) \text{ for all } a \in \mathbf{Z}_p \\ &\iff p(x)\big|f(x) \iff f(x) \in \big\langle p(x) \big\rangle = \langle x^p - x \rangle. \end{aligned}$$

Furthermore, we claim that ϕ is surjective. For $a \in \mathbf{Z}_p$, let $g_a(x) \in \mathbf{Z}_p[x]$ be the polynomial

$$g_a(x) = \frac{\prod\limits_{i \in \mathbf{Z}_p, i \neq a} (x - i)}{\prod\limits_{i \in \mathbf{Z}_p, i \neq a} (a - i)}\,.$$

Notice that for all $k \in \mathbf{Z}_p$ we have

$$g_a(k) = \delta_{a,k} = \begin{cases} 1 \text{ if } k = a, \\ 0 \text{ if } k \neq a. \end{cases}$$

Given any function $f(x) \in \text{Func}(\mathbf{Z}_p, \mathbf{Z}_p)$, for all $k \in \mathbf{Z}_p$ we have

$$\sum_{a \in \mathbf{Z}_p} f(a) g_a(k) = \sum_{a \in \mathbf{Z}_p} f(a) \delta_{a,k} = f(k).$$

It follows that $f(x) = \sum\limits_{a \in \mathbf{Z}_p} f(a) g_a(x) \in \text{Func}(\mathbf{Z}_p, \mathbf{Z}_p)$. Notice that $\sum\limits_{a \in \mathbf{Z}_p} f(a) g_a(x) \in \mathbf{Z}_p[x]$ and we have $f(x) = \phi\Big(\sum\limits_{a \in \mathbf{Z}_p} f(a) g_a(x)\Big)$. Thus ϕ is surjective, as claimed. Thus the ring of polynomial functions $\phi\big(\mathbf{Z}_p[x]\big)$ is equal to the ring of all functions $\text{Func}(\mathbf{Z}_p, \mathbf{Z}_p)$, and by the First Isomorphism Theorem, we have $\mathbf{Z}_p[x]\big/\langle x^p - x \rangle \cong \phi\big(\mathbf{Z}_p[x]\big) = \text{Func}(\mathbf{Z}_p, \mathbf{Z}_p)\,.$

.

Chapter 10. Factorization in Commutative Rings

10.1 Definition: Let R be a ring. An ideal P in R is called **prime** when $P \neq R$ and for all ideals A and B in R, if $AB \subseteq P$ then either $A \subseteq P$ or $B \subseteq P$. An ideal M in R is called **maximal** when $M \neq R$ and there is no ideal A in R with $M \subsetneqq A \subsetneqq R$.

10.2 Example: As an exercise, use the above definition to show that the maximal ideals in $\mathbf{Z}$ are the ideals of the form $\langle p \rangle$ with p prime, and the prime ideals in $\mathbf{Z}$ are the ideals of the form $\langle p \rangle$ with $p = 0$ or p prime.

10.3 Theorem: *Let R be a commutative ring with 1. Let P be an ideal in R with $P \neq R$. Then P is prime if and only if P has the property that for all $a, b \in R$, if $ab \in P$ then either $a \in P$ or $b \in P$.*

Proof: Since R is commutative with 1, we have $\langle a \rangle = \{ar \big| r \in R\}$ and $\langle b \rangle = \{bs \big| s \in R\}$ and so

$$\begin{aligned}\langle a \rangle \langle b \rangle &= \Big\{ \sum_{i=1}^{n} a_i b_i \Big| a_i \in \langle a \rangle, b_i \in \langle b \rangle \Big\} = \Big\{ \sum_{i=1}^{n} (ar_i)(bs_i) \Big| r_i, s_i \in R \Big\} \\ &= \Big\{ \sum_{i=1}^{n} (ab)t_i \Big| t_i \in R \Big\} = \langle ab \rangle.\end{aligned}$$

Suppose that P is prime. Let $a, b \in R$ with $ab \in P$. Then $\langle a \rangle \langle b \rangle = \langle ab \rangle \subseteq P$ and so, since P is prime, either $\langle a \rangle \subseteq P$ or $\langle b \rangle \subseteq P$, and hence either $a \in P$ or $b \in P$.

Conversely, suppose that P has the property that for all $a, b \in R$, if $ab \in P$ then either $a \in P$ or $b \in P$. Let A and B be ideals in R with $AB \subseteq P$. Suppose that $A \not\subseteq P$. Choose $a \in A$ with $a \notin P$. Let $b \in B$ be arbitrary. Then $ab \in AB \subseteq P$ and so, because of the property held by P, either $a \in P$ or $b \in P$. Since $a \notin P$ we must have $b \in P$. Thus $B \subseteq P$.

10.4 Theorem: *Let R be a commutative ring with 1. Let P be an ideal in R. Then P is prime if and only if R/P is an integral domain.*

Proof: Suppose that P is prime. Since $P \neq R$ we have $1 \notin P$ (since $\langle 1 \rangle = R$) and so $1 + P \neq 0 + P \in P/R$. Since R is commutative, so is R/P. Finally, note that R/P has no zero divisors because for $a, b \in R$ we have

$$\begin{aligned}(a+P)(b+P) = (0+P) &\Longrightarrow ab + P = 0 + P \Longrightarrow ab \in P \Longrightarrow a \in P \text{ or } b \in P \\ &\Longrightarrow a + P = 0 + P \text{ or } b + P = 0 + P.\end{aligned}$$

Conversely, suppose that R/P is an integral domain. Since $1 + P \neq 0 + P \in R/P$, it follows that $1 \notin P$ and so $P \neq R$. Let $a, b \in R$ with $ab \in P$. Then we have $ab + P = 0 + P$, and so $(a+P)(b+P) = 0 + P$. Since R/P has no zero divisors, this implies that either $a + P = 0 + P$ or $b + P = 0 + P$, and so either $a \in P$ or $b \in P$.

10.5 Example: Let R be a commutative ring with 1. Show that every maximal ideal in R is also prime.

Solution: Let M be a maximal ideal in R. Let $a, b \in R$ with $ab \in M$. Suppose that $a \notin M$. Then we have $M \subsetneqq M + \langle a \rangle$ and so, since M is maximal, we must have $M + \langle a \rangle = R$. In particular $1 \in M + \langle a \rangle$, so we have $1 = m + ar$ for some $r \in R$. Thus

$$b = b \cdot 1 = b(m + ar) = bm + ab\,r \in M\,.$$

We remark that this result also follows from the following theorem.

10.6 Theorem: *Let R be a commutative ring with 1. Let M be an ideal in R. Then M is maximal if and only if R/M is a field.*

Proof: Suppose M is maximal. Since $M \neq R$ we have $1 \notin M$ and so $1+M \neq 0+M \in R/M$. Since R is commutative, so is R/M. Let $a+M$ be a nonzero element in R/M. We must show that $a+M$ is a unit. Since $a+M \neq 0+M$ we have $a \notin M$. Since $a \notin M$ we have $M \subsetneqq M+\langle a\rangle$. Since M is maximal, we must have $M+\langle a\rangle = R$. In particular, $1 \in M+\langle a\rangle$, say $1 = m+ar$ with $r \in R$. Then $1+M = ar+M = (a+M)(r+M)$ and so $r+M$ is the inverse of $a+M$.

Conversely, suppose that R/M is a field. Since $1+M \neq 0+M$ in R/M, we have $1 \notin M$ so $M \neq R$. Let A be an ideal with $M \subseteq A \subseteq R$. Suppose $A \neq M$. Choose $a \in A$ with $a \notin M$. Since $a \notin M$ we have $a+M \neq 0+M$ in R/M. Since R/M is a field, $a+M$ has an inverse, say $(a+M)(b+M) = 1+M$. Then $ab+M = 1+M$ so we have $1-ab \in M$. Since $M \subseteq A$ we have $1-ab \in A$. Since $a \in A$ we have $ab \in A$, so $1 \in A$ and hence $A = R$.

10.7 Example: Find all prime and maximal ideals in $\mathbf{Z}$ (that is redo example 10.2) using Theorems 10.4 and 10.6.

10.8 Example: Since $\mathbf{Q}[x]/\langle x^2-2\rangle \cong \mathbf{Q}[\sqrt{2}]$, which is a field, it follows that $\langle x^2-2\rangle$ is maximal (and prime). In $\mathbf{R}[x]$, however, we have $(x^2-2) = (x-\sqrt{2})(x+\sqrt{2})$, and so the ideal $\langle x^2-2\rangle$ is not maximal because $\langle x^2-2\rangle \subsetneqq \langle x-\sqrt{2}\rangle \subsetneqq \mathbf{R}[x]$ and it is not prime because $(x-\sqrt{2})(x+\sqrt{2}) \in \langle x^2-2\rangle$ but $(x-\sqrt{2}) \notin \langle x^2-2\rangle$ and $(x+\sqrt{2}) \notin \langle x^2-2\rangle$.

10.9 Example: In $\mathbf{Z}[x]$, we have $\langle x\rangle = \big\{f \in \mathbf{Z}[x] \big| f(0) = 0\big\}$. The ideal $\langle x\rangle$ is prime because for $f,g \in \mathbf{Z}[x]$, if $fg \in \langle x\rangle$ then $f(0)g(0) = 0$ and so either $f(0) = 0$ or $g(0) = 0$. But the ideal $\langle x\rangle$ is not maximal since $\langle x\rangle \subsetneqq \langle 2,x\rangle = \big\{f \in \mathbf{Z}[x] \big| f(0) \text{ is even}\big\} \subsetneqq \mathbf{Z}[x]$.

10.10 Definition: Let R be a commutative ring with 1. Let $a,b \in R$. We say that a **divides** b (or that a is a **divisor** or **factor** of b, or that b is a **multiple** of a), and we write $a\big|b$, when $b = ar$ for some $r \in R$. We say that a and b are **associates**, and we write $a \sim b$, when $a\big|b$ and $b\big|a$. Note that association is an equivalence relation on R.

10.11 Theorem: *Let R be a commutative ring with 1. Let $a,b \in R$. Then*
(1) $a\big|b$ if and only if $b \in \langle a\rangle$ if and only if $\langle b\rangle \subseteq \langle a\rangle$,
(2) $a \sim b$ if and only if $\langle a\rangle = \langle b\rangle$ if and only if a and b have the same multiples and divisors,
(3) $a \sim 0$ if and only if $a = 0$ if and only if $\langle a\rangle = \{0\}$,
(4) $a \sim 1$ if and only if a is a unit if and only if $\langle a\rangle = R$.
(5) if R is an integral domain then $a \sim b$ if and only if $b = au$ for some unit $u \in R$.

Proof: We prove Part (5) and leave the other proofs as an exercise. Suppose that $b = au$ where $u \in R$ is a unit. Since $b = au$ we have $a|b$ and since $a = bu^{-1}$ we have $b|a$. Since $a|b$ and $b|a$ we have $a \sim b$ (we did not need to assume that R is an integral domain for this direction). Now suppose that R is an integral domain and that $a \sim b$, say $a = br$ and $b = as$ with $r,s \in R$. Then we have $b = as = brs$ so that $b(1-rs) = 0$. Since R is an integral domain, either $b = 0$ or $1-rs = 0$. If $b = 0$ then $a = br = 0$, so we have $b = a \cdot u$ for any unit u (for example $u = 1$). If $1-rs = 0$ then $rs = 1$ so that r and s are units, so we have $b = au$ where $u = s$ (which is a unit).

10.12 Example: In the ring $\mathbf{Z}$, we have $k \sim \ell \iff k = \pm\ell$. Verify that in $\mathbf{Z}_{12}$ the association classes are $\{0\}$, $\{1,5,7,11\}$, $\{2,10\}$, $\{3,9\}$, $\{4,8\}$, $\{6\}$.

10.13 Definition: Let R be a commutative ring with 1. Let $a \in R$ be a non-zero non-unit. We say that a is **reducible** when $a = bc$ for some non-units $b, c \in R$, and otherwise we say that a is **irreducible**. We say that a is **prime** when for all $b, c \in R$, if $a \big| bc$ then either $a \big| b$ or $a \big| c$.

10.14 Theorem: *Let R be a commutative ring with 1. Let $a, b \in R$ with $a \sim b$. Then*
(1) $a = 0$ if and only if $b = 0$,
(2) a is a unit if and only if b is a unit,
(3) a is reducible if and only if b is reducible,
(4) a is irreducible if and only if b is irreducible,
(5) a is prime if and only if b is prime.

Proof: The proof is left as an exercise.

10.15 Example: In the ring $\mathbf{Z}$, for $k \in \mathbf{Z}$, k is irreducible if and only if k is prime if and only if $k = \pm p$ for some (positive) prime number p.

10.16 Example: As an exercise, verify that in the ring $\mathbf{Z}_{12}$, the irreducible elements are 2 and 10 and the prime elements are 2, 3, 9 and 10.

10.17 Example: Use the method of the Sieve of Eratosthenes to find several irreducible elements in $\mathbf{Z}[\sqrt{3}\, i]$ and also some irreducible elements which are not prime.

10.18 Theorem: *Let R be a commutative ring with 1. Let $a \in R$. Then*
(1) If a is irreducible then the divisors of a are the units in R and the associates of a in R.
(2) a is prime if and only if $\langle a \rangle$ is a non-zero prime ideal.

Proof: The proof is left as an exercise.

10.19 Theorem: *Let R be an integral domain and let $a \in R$. Then*
(1) if a is prime then a is irreducible,
(2) a is irreducible if and only if $\langle a \rangle$ is maximal amongst non-zero proper principal ideals,
(3) if R is a PID and a is irreducible, then a is prime.

Proof: To Prove Part (1), suppose that a is prime. Suppose that $a = bc$ with $b, c \in R$. Since $a = bc$ we have $a \big| bc$ and hence, since a is prime, either $a|b$ or $a|c$. Suppose that $a|b$, say $b = ar$. Then $a = bc = arc$ so that $a(1 - rc) = 0$. Since R is an integral domain and $a \neq 0$ it follows that $rc = 1$ so that c is a unit. A similar argument shows that if $a|c$ then b is a unit, and so a is irreducible, as required.

To prove Part (2), suppose that a is irreducible. Since $a \neq 0$ we have $\langle a \rangle \neq 0$ and since a is not a unit we have $\langle a \rangle \neq R$. Let $b \in R$ and suppose that $\langle a \rangle \subseteq \langle b \rangle \subseteq R$. Since $\langle a \rangle \subseteq \langle b \rangle$ we have $a \in \langle b \rangle$, say $a = bc$ with $c \in \mathbf{R}$. Since a is irreducible, either b is a unit, in which case $\langle b \rangle = R$, or c is a unit in which case $b \sim a$ so that $\langle b \rangle = \langle a \rangle$.

Suppose, conversely, that $\langle a \rangle$ is maximal amongst nonzero proper principal ideals in R. Since $\langle a \rangle \neq \{0\}$ we have $a \neq 0$ and since $\langle a \rangle \neq R$ it follows that a is not a unit. Suppose that $a = bc$ where $b, c \in R$. Since $a = bc$ we have $a \in \langle b \rangle$ so that $\langle a \rangle \subseteq \langle b \rangle$. By the maximality of $\langle a \rangle$, either $\langle b \rangle = \langle a \rangle$ or $\langle b \rangle = R$. If $\langle b \rangle = R$ then b is a unit. Suppose that $\langle b \rangle = \langle a \rangle$, say $b = ar$ with $r \in R$. Then $a = bc = arc$ so that $a(1 - rc) = 0$. Since $a(1 - rc) = 0$ and $a \neq 0$ and R is an integral domain, it follows that $rc = 1$ so that c is a unit. This completes the proof of Part (2).

Finally note that if a is irreducible and R is a PID then, by Part (2), $\langle a \rangle$ is a maximal ideal, hence $\langle a \rangle$ is a prime ideal, hence a is prime. This proves Part (3).

10.20 Definition: A **Euclidean domain** (or ED) is an integral domain R together with a function $N : R \setminus \{0\} \to \mathbf{N}$, called a **norm**, with the property that for all $a, b \in R$ with $a \neq 0$ there exist $q, r \in R$ such that $b = qa + r$ and either $r = 0$ or $N(r) < N(a)$.

10.21 Definition: A **principal ideal domain** (or PID) is an integral domain R such that every ideal in R is principal.

10.22 Definition: A **unique factorization domain** (or UFD) is an integral domain R with the property that for every nonzero non-unit $a \in R$ we have
(1) $a = a_1 a_2 \cdots a_l$ for some $l \in \mathbf{Z}^+$ and some irreducible elements $a_i \in R$, and
(2) if $a = a_1 a_2 \cdots a_l = b_1 b_2 \cdots b_m$ where $l, m \in \mathbf{Z}^+$ and each a_i and b_j is irreducible, then $m = l$ and for some permutation $\sigma \in S_m$ we have $a_i \sim b_{\sigma(i)}$ for all i.

10.23 Example: The ring $\mathbf{Z}$ is a Euclidean domain with norm given by $N(k) = |k|$.

10.24 Example: Every field F is a Euclidean domain, using any function $N : F \setminus \{0\} \to \mathbf{N}$ as a norm. Indeed, given $a, b \in F$ with $a \neq 0$ we can choose $q = \frac{b}{a}$ and $r = 0$ to get $b = aq + r$.

10.25 Example: If F is a field then $F[x]$ is a Euclidean domain with norm $N(f) = \deg(f)$.

10.26 Example: Show that in the ring $\mathbf{Z}[\sqrt{3}\,i]$, the elements 2 and $1 \pm \sqrt{3}\,i$ are irreducible and $2 \not\sim 1 \pm \sqrt{3}\,i$. It follows that $\mathbf{Z}[\sqrt{3}\,i]$ not a unique factorization domain because $4 = 2 \cdot 2 = (1 + \sqrt{3}\,i)(1 - \sqrt{3}\,i)$.

10.27 Theorem: *Every Euclidean domain is a principal ideal domain.*

Proof: Let R be a Euclidean domain with norm N. Let A be an ideal in R. If $A = \{0\}$ then A is principal with $A = \langle 0 \rangle$. Suppose that $A \neq \{0\}$. Choose a nonzero element $0 \neq a \in A$ of smallest possible norm. We claim that $A = \langle a \rangle$. Since $a \in A$ we have $\langle a \rangle \subseteq A$. Let $b \in A$ be arbitrary. Choose $q, r \in R$ such that $b = qa + r$ and either $r = 0$ or $N(r) < N(a)$. Note that $r = b - qa \in A$ so we must have $r = 0$ by the choice of a. Thus $b = qa \in \langle a \rangle$.

10.28 Definition: A ring R is called **Noetherian** when it satisfies the following condition, which is called the **ascending chain condition**: for every ascending chain of ideals $A_1 \subseteq A_2, \subseteq A_3 \subseteq \cdots$ in R, there exists $n \in \mathbf{Z}^+$ such that $A_k = A_n$ for all $k \geq n$.

10.29 Theorem: *Every principal ideal domain is Noetherian.*

Proof: Let R be a principal ideal domain. Let $a_1, a_2, a_3, \cdots \in R$ with

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots .$$

Let $A = \bigcup_{k=1}^{\infty} \langle a_k \rangle$. Verify that A is an ideal. Choose $a \in R$ so that $A = \langle a \rangle$. Since $a \in A$, we can choose $n \in \mathbf{Z}^+$ so that $a \in \langle a_n \rangle$. For all $k \geq n$, we have $\langle a_k \rangle \subseteq A = \langle a \rangle \subseteq \langle a_n \rangle \subseteq \langle a_k \rangle$ and so $\langle a_k \rangle = \langle a_n \rangle$.

10.30 Theorem: *Every principal ideal domain is a unique factorization domain.*

Proof: Let R be a principal ideal domain. Let $a \in R$ be a non-zero non-unit. We claim that a has an irreducible factor. If a is irreducible then we are done. Suppose that a is reducible, say $a = a_1 b_1$ where a_1 and b_1 are non-units. Note that $\langle a \rangle \subsetneqq \langle a_1 \rangle$. If a_1 is irreducible then we are done. Suppose that a_1 is reducible, say $a_1 = a_2 b_2$ where a_2 and b_2 are non-units. Then $a = a_1 b_1 = a_2 b_2 b_1$ and $\langle a \rangle \subsetneqq \langle a_1 \rangle \subsetneqq \langle a_2 \rangle$. If a_2 is irreducible then we are done, and otherwise we continue this procedure. Eventually, the procedure must end giving us an irreducible factor a_n of a, otherwise we would obtain an infinite chain of ideals $\langle a \rangle \subsetneqq \langle a_1 \rangle \subsetneqq \langle a_2 \rangle \subsetneqq \cdots$, contradicting the fact that R is Noetherian.

Next we claim that $a = a_1 a_2 \cdots a_l$ for some $l \in \mathbf{Z}^+$ and some irreducible $a_i \in R$. If a is irreducible then we are done. Suppose that a is reducible. Let a_1 be an irreducible factor of a, and say $a = a_1 b_1$. Note that b_1 is not a unit since, if it was then we would have $a \sim a_1$, but a is reducible and a_1 is not. If b_1 is irreducible then we are done. Suppose b_1 is reducible. Let a_2 be an irreducible factor of b_1 and say $b_1 = a_2 b_2$. As above, note that b_2 is not a unit. If b_2 is irreducible then we are done, and otherwise we continue the procedure. Eventually, the procedure must end giving us $a = a_1 a_2 \cdots a_n b_n$ with each a_i and n_n irreducible, otherwise we would obtain an infinite chain $\langle a \rangle \subsetneqq \langle b_1 \rangle \subsetneqq \langle b_2 \rangle \subsetneqq \cdots$.

Finally, we claim that if $a = a_1 a_2 \cdots a_l = b_1 b_2 \cdots b_l$ with $l, m \in \mathbf{Z}^+$ and each a_i and b_j irreducible, then $m = l$ and for some permutation $\sigma \in S_m$ we have $a_i \sim b_{\sigma(i)}$ for all i. Suppose that $a = a_1 a_2 \cdots a_l = b_1 b_2 \cdots b_m$ where $l, m \in \mathbf{Z}^+$ and the a_i and b_j are irreducible. Since $a_1 \big| a_1 a_2 \cdots a_l$, we have $a_1 \big| b_1 b_2 \cdots b_m$. Since a_1 is irreducible and R is a principal ideal domain, it follows that a_1 is prime by Part 3 of Theorem 10.19. Since a_1 is prime and $a_1 \big| b_1 b_2 \cdots b_m$, it follows that $a_1 \big| b_k$ for some k. After permuting the elements b_i we can assume $a_1 \big| b_1$. Since b_1 is irreducible, its divisors are units and associates and, since a_1 is not a unit, we have $a_1 \sim b_1$. Since $a_1 \sim b_1$ we have $b_1 = a_1 u$ for some unit u. Thus we have $a_1 a_2 \cdots a_l = b_1 b_2 \cdots b_m = a_1 u b_2 b_3 \cdots b_m$, and by cancellation, $a_2 a_3 \cdots a_l = u b_2 b_3 \cdots b_m$. A suitable induction argument gives $l = m$ and $a_i \sim b_i$ for all i.

10.31 Example: Show that $\mathbf{Z}[i]$ is a ED.

10.32 Example: Since $\mathbf{Z}[\sqrt{3}\, i]$ is not aUFD, it cannot be a PID. Find an ideal in $\mathbf{Z}[\sqrt{3}\, i]$ which is not principal.

10.33 Example: Show that $\mathbf{Z}\left[\frac{1+\sqrt{19}\, i}{2}\right]$ is a PID, but not a ED (under any norm).

.

Chapter 11. Polynomial Rings

11.1 Note: Here are a few remarks about polynomials. Recall that $R[x]$ denotes the ring of polynomials with coefficients in the ring R, and R^R denotes the ring of all functions $f : R \to R$.

(1) A polynomial $f \in R[x]$ determines a function $f \in R^R$. Given $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ we obtain the function $f : R \to R$ given by $f(x) = \sum_{i=0}^{n} a_i x^i$.

(2) Although we do not usually distinguish notationally between the polynomial $f \in R[x]$ and its corresponding function $f \in R^R$, they are not always identical. If the ring R is not commutative then multiplication of polynomials does not agree with multiplication of functions. For $f, g \in R[x]$ given by $f(x) = a + bx$ and $g(x) = c + dx$, in the ring $R[x]$ we have $(fg)(x) = (a+bx)(c+dx) = (ac) + (ad+bc)x + (bd)x^2$, but in the ring R^R we have $(fg)(x) = (a+bx)(c+dx) = ac + adx + bxc + bxdx$.

(3) Equality of polynomials may not agree with equality of functions. For $f, g \in R[x]$ given by $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ we have $f = g \in R[x]$ if and only if $a_i = b_i$ for all i (and if say $n < m$ then $b_i = a_i = 0$ for $i > n$), but $f = g \in R^R$ if and only if $f(x) = g(x)$ for all $x \in R$. These two notions of equality do not always agree. For example if R is finite then the ring $R[x]$ is infinite but the ring R^R is finite. Indeed if $|R| = n$ then $R[x]$ is countably infinite but $\left|R^R\right| = n^n$. For a more specific example, if $f(x) = x^p - x$ then we have $f \neq 0 \in \mathbf{Z}_p[x]$ (because its coefficients are not equal to zero) but $f = 0 \in {\mathbf{Z}_p}^{\mathbf{Z}_p}$ because, by Fermat's Little Theorem, we have $f(x) = 0$ for all $x \in \mathbf{Z}_p$.

(4) Recall that for $f(x) = \sum_{i=0}^{n} a_i x^i$ with each $a_i \in R$ and $a_n \neq 0$, the element $a_n \in R$ is called the leading coefficient of f, and the non-negative integer n is called the degree of $f(x)$, and we write $\deg(f) = n$. For convenience, we also define $\deg(0) = -1$. When R is an integral domain, it is easy to see that for $0 \neq f, g \in R[x]$ we have $\deg(fg) = \deg(f) + \deg(g)$. When R is not an integral domain, however, we only have $\deg(fg) \leq \deg(f) + \deg(g)$ because the product of the two leading coefficients can be equal to zero.

(5) When R is an integral domain, because we have $\deg(fg) = \deg(f) + \deg(g)$ for all $0 \neq f, g \in R[x]$, it is easy to see that the units in $R[x]$ are the constant polynomials $f(x) = c$ where c is a unit in R. In particular, when F is a field, the units in $F[x]$ are the elements $f \in F[x]$ with $\deg(f) = 0$. In the ring $\mathbf{Z}_4[x]$ (which is not an integral domain) we have $(1+2x)^2 = 1 + 4x + 4x^2 = 1$, so $f(x) = (1+2x)$ is a unit in $\mathbf{Z}_4[x]$.

11.2 Theorem: (*Division Algorithm*) *Let R be a ring. Let $f, g \in R[x]$ and suppose that the leading coefficient of g is a unit in R. Then there exist unique polynomials $q, r \in R$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.*

Proof: First we prove existence. If $\deg(f) < \deg(g)$ then we can take $q = 0$ and $r = f$. Suppose that $\deg(f \geq \deg(g)$, Say $f(x) = \sum\limits_{i=0}^{n} a_i x^i$ with $a_i \in R$ and $a_n \neq 0$ and $g(x) = \sum\limits_{i=0}^{m} b_i x^i$ with $b_i \in R$ and b_m is a unit. Note that the polynomial $a_n {b_m}^{-1} x^{n-m} g(x)$ has degree n and leading coefficient a_n. It follows that the polynomial $f(x) - a_n {b_m}^{-1} x^{n-m} g(x)$ has degree smaller than n (because the leading coefficients cancel). We can suppose, inductively, that there exist polynomials $p, r \in R[x]$ such that $f(x) - a_n {b_m}^{-1} x^{n-m} g(x) = p(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$. Then we have $f = qg + r$ by taking $q(x) = a_n {b_m}^{-1} x^{n-m} - p(x)$.

Next we prove uniqueness. Suppose that $f = qg + r = pg + s$ where $q, p, r, s \in R[x]$ with $\deg(r) < \deg(g)$ and $\deg(s) < \deg(g)$. Then we have $(q-p)g = s - r$ and so $\deg\big((q-p)g\big) = \deg(s-r)$. Since the leading coefficient of g is a unit (hence not a zero divisor), it follows that $\deg\big((q-p)g\big) = \deg(q-p) + \deg(g)$. If we had $q - p \neq 0$ then we would have $\deg\big((q-p)g\big) \geq \deg(g)$ but $\deg(s-r) < \deg(g)$, giving a contradiction. Thus we must have $q - p = 0$. Since $q - p = 0$ we have $s - r = (q-p)g = 0$. Since $q - p = 0$ and $s - r = 0$ we have $q = p$ and $r = s$, proving uniqueness.

11.3 Corollary: (*The Remainder Theorem*) *Let R be a ring, let $f \in R[x]$, and let $a \in R$. When we divide $f(x)$ by $(x-a)$ to obtain the quotient $q(x)$ and remainder $r(x)$, the remainder is the constant polynomial $r(x) = f(a)$.*

Proof: Use the division algorithm to obtain $q, r \in R[x]$ such that $f = q(x)(x-a) + r(x)$ and $\deg(r) < \deg(x-a)$. Since $\deg(x-a) = 1$ we have $\deg(r) \in \{-1, 0\}$, and so r is a constant polynomial, say $r(x) = c$ with $c \in R$. Then we have $f(x) = q(x)(x-a) + c$. Put in $x = a$ to get $f(a) = q(a)(a-a) + c = q(a) \cdot 0 + c = c$.

11.4 Corollary: (*The Factor Theorem*) *Let R be a commutative ring, let $f \in R[x]$ and let $a \in R$. Then $f(a) = 0$ if and only if $(x-a)\big|f(x)$.*

Proof: Suppose that $f(a) = 0$. Choose $q, r \in R[x]$ such that $f(x) = q(x)(x-a) + r(x)$ and $\deg(r) < \deg(x-a)$. Then $r(x)$ is the constant polynomial $r(x) = f(a) = 0$ and so we have $f(x) = q(x)(x-a)$. Since $f(x) = (x-a)q(x)$ we have $(x-a)\big|f(x)$. Conversely, suppose that $(x-a)\big|f(a)$ and choose $p \in R[x]$ so that $f(x) = (x-a)p(x)$. Then $f(a) = (a-a)p(a) = 0 \cdot p(a) = 0$.

11.5 Definition: Let R be a commutative ring, let $f \in R[x]$, and let $a \in R$. We say that a is a **root** of f when $f(a) = 0$. When $f \neq 0$, we define the **multiplicity** of a as a root of f to be the largest $m = m(f, a) \in \mathbf{N}$ such that $(x-a)^m\big|f(x)$ (where we use the convention that $(x-a)^0 = 1$). Note that a is a root of f if and only if $m(f, a) \geq 1$.

11.6 Example: Let $f(x) = x^3 - 3x - 2 \in \mathbf{Q}[x]$. Since $f(x) = (x+1)^2(x-2) \in \mathbf{Q}[x]$, we have $m(f, 2) = 1$ and $m(f, -1) = 2$.

11.7 Example: Let p be an odd prime and let $f(x) = x^p - a \in \mathbf{Z}_p[x]$. Find $m(f, a)$.

11.8 Theorem: (*The Roots Theorem*) *Let R be an integral domain, let $0 \neq f \in R[x]$ and let $n = \deg(f)$. Then*

(1) f has at most n distinct roots in R, and
(2) if $a_1, a_2, \cdots, a_\ell$ are all of the distinct roots of f in R and $m_i = m(f, a_i)$ for $1 \leq i \leq \ell$, then $(x - a_1)^{m_1}(x - a_2)^{m_2} \cdots (x - a_\ell)^{m_\ell} \big| f(x)$ and so $\sum\limits_{i=1}^{\ell} m(f, a) \leq n$.

Proof: We prove Part (1) and leave the proof of Part (2) as an exercise. If $\deg(f) = 0$, then $f(x) = c$ for some $0 \neq c \in R$, and so $f(x)$ has no roots. Let f be a polynomial with $\deg(f) = n \geq 1$ and suppose, inductively, that every polynomial $g \in R[x]$ with $\deg(g) = n - 1$ has at most $n - 1$ distinct roots. Suppose that a is a root of f in R. By the Factor Theorem, $(x - a)\big|f(x)$ so we can choose a polynomial $g \in R[x]$ so that $f(x) = (x - a)g(x)$. Note that $\deg(g) = n - 1$ so, by the induction hypothesis, g has at most $n-1$ distinct roots. Let $b \in R$ be any root of f with $b \neq a$. Since $f(x) = (x-a)g(x)$ and $f(b) = 0$ we have $0 = f(b) = (b - a)g(b)$. Since $(b-a)g(b) = 0$ and $(b-a) \neq 0$ and R has no zero divisors, it follows that $g(b) = 0$. Thus b must be one of the roots of g. Since every root b of f with $b \neq a$ is equal to one of the roots of g, and since g has at most $n-1$ distinct roots, it follows that f has at most n distinct roots, as required.

11.9 Example: When R is not an integral domain, a polynomial $f \in R[x]$ of degree n can have more than n roots. For example, in the ring $\mathbf{Z}_6[x]$ the polynomial $f(x) = x^2 + x$ has roots 0, 2, 3 and 5.

11.10 Theorem: (*The Rational Roots Theorem*) *Let $f(x) = \sum\limits_{i=0}^{n} c_i x^i \in \mathbf{Z}[x]$ where $n \in \mathbf{Z}^+$ and $c_n \neq 0$. Let $r, s \in \mathbf{Z}$ with $s \neq 0$ and $\gcd(r, s) = 1$. Then if $f\left(\frac{r}{s}\right) = 0$ then $r|c_0$ and $s|c_n$.*

Proof: Suppose that $f\left(\frac{r}{s}\right) = 0$, that is $c_0 + c_1 \frac{r}{s} + c_2 \frac{r^2}{s^2} + \cdots + c_n \frac{r^n}{s^n} = 0$. Multiply by s^n to get

$$0 = c_0 s^n + c_1 s^{n-1} r^1 + \cdots + c_{n-1} s^1 r^{n-1} + c_n r^n.$$

Thus we have

$$\begin{aligned} c_0 s^n &= -r(c_1 s^{n-1} + \cdots + c_{n-1} s^1 r^{n-2} + c_n r^{n-1}) \text{ and} \\ c_n r^n &= -s\big(c_0 s^{n-1} + c_1 s^{n-2} r^1 + \cdots + c_{n-1} r^{n-1}\big) \end{aligned}$$

and it follows that $r\big|c_0 s^n$ and that $s\big|c_n r^n$. Since $\gcd(r, s) = 1$ we also have $\gcd(r, s^n) = 1$, and since $r\big|c_0 s^n$ it follows that $r|c_0$. Since $\gcd(s, r) = 1$ we also have $\gcd(s, r^n) = 1$, and since $s\big|c_n r^n$ it follows that $s|c_n$.

11.11 Example: Show that $\sqrt{1 + \sqrt{2}} \notin \mathbf{Q}$.

11.12 Note: Here are a few remarks about irreducible polynomials.

(1) When F is a field, we know that $F[x]$ is a unique factorization domain. For $f \in F[x]$ we know that $f = 0$ if and only if $\deg(f) = -1$, and f is a unit if and only if $\deg(f) = 0$, and for $0 \neq f, g \in F[x]$ we know that $\deg(fg) = \deg(f) + \deg(g)$. It follows that for $f \in F[x]$, if $\deg(f) = 1$ then f is irreducible. It also follows that for $f \in F[x]$, if $\deg(f) = 2$ or 3 then f is reducible in $F[x]$ if and only if f has a f has a root in F.

(2) For $f \in \mathbf{C}[x]$, we know (from the Fundamental Theorem of Algebra) that f is irreducible if and only if $\deg(f) = 1$. For $f \in \mathbf{R}[x]$, we know that f is irreducible polynomial if and only if either $\deg(f) = 1$ or $f(x) = ax^2 + bx + c$ for some $a, b, c \in \mathbf{R}$ with $a \neq 0$ and $b^2 - 4ac < 0$.

(3) When p is a fairly small prime number and n is a fairly small positive integer, it is easy to list all reducible and irreducible polynomials $f \in \mathbf{Z}_p[x]$ with $\deg(f) \leq n$. Note that it suffices to list monic polynomials (since for $f \in \mathbf{Z}_p[x]$ and $0 \neq c \in \mathbf{Z}_p[x]$ we have $f \sim cf$). We start by listing all monic polynomials of degree 1, that is all polynomials of the form $f(x) = x + a$ with $a \in \mathbf{Z}_p$, and noting that they are all irreducible. Having constructed all reducible and irreducible monic polynomials of all degrees less than n, we can construct all of the reducible monic polynomials of degree n by forming products of the reducible monic polynomials of smaller degree in all possible ways, and then all the remaining monic polynomials of degree n must be irreducible.

11.13 Example: Note that $f(x) = x^3 - 3x + 1$ is irreducible in $\mathbf{Q}[x]$ because it is cubic and has no roots in $\mathbf{Q}$ by the Rational Roots Theorem. The same polynomial is reducible in $\mathbf{R}[x]$ and in $\mathbf{C}[x]$ because it is cubic.

11.14 Example: List all monic reducible and irreducible polynomials in $\mathbf{Z}_2[x]$ of degree less than 4, then determine the number of irreducible polynomials in $\mathbf{Z}_2[x]$ of degree 4.

11.15 Definition: Let R be an integral domain. Define a binary relation on the set $R \times (R \setminus \{0\})$ by stipulating that

$$(a, b) \sim (b, d) \iff ad = bc.$$

It is easy to check that this is an equivalence relation. Let

$$F = Q(R) = \big(R \times (R \setminus \{0\})\big)\Big/\!\sim\; = \Big\{[(a, b)]\Big| a, b \in R, b \neq 0\Big\}.$$

Define addition an multiplication operations on F by

$$\begin{aligned} \big[(a, b)\big] + \big[(c, d)\big] &= \big[(ad + bc\,,\, bd)\big], \\ \big[(a, b)\big]\,\big[(c, d)\big] &= \big[(ac\,,\, bd)\big]. \end{aligned}$$

It is not hard to verify that these operations are well-defined (noting that when $b \neq 0$ and $d \neq 0$ we also have $bd \neq 0$ because R is an integral domain) and that they make F into a field with zero element $[(0, 1)]$ and identity element $[(1, 1)]$. This field $F = Q(R)$ is called the **quotient field** of the integral domain R. For $a, b \in R$ with $b \neq 0$ we use the following notation:

$$\tfrac{a}{b} = [(a, b)]\ ,\ a = [(a, 1)]\ ,\ \tfrac{1}{b} = [(1, b)].$$

The use of the notation $a = [(a, 1)]$, for $a \in R$, allows to consider R as a subring of its quotient field F.

11.16 Example: The quotient field of $\mathbf{Z}$ is equal to $\mathbf{Q}$, and the quotient field of $\mathbf{Z}[\sqrt{2}]$ is equal to $\mathbf{Q}[\sqrt{2}]$.

11.17 Example: When R is an integral domain, the quotient field of the polynomial ring $R[x]$ is the **field of rational functions** $R(x) = \left\{ \frac{f}{g} \,\middle|\, f, g \in R[x], g \neq 0 \right\}$. More generally, the quotient field of $R[x_1, \cdots, x_n]$ is the field of rational functions $R(x_1, \cdots, x_n)$.

11.18 Definition: Let R be a unique factorization domain. For a polynomial $f \in R[x]$, the **content** of f, written as $c(f)$, is a greatest common divisor of the coefficients of f. Note that the greatest common divisor is unique up to association and so $c(f)$ is unique up to association, that is up to multiplication by a unit. We often abuse notation by writing $c(f) = a$ when in fact $c(f) \sim a$. We say that f is **primitive** when $c(f) = 1$ (that is when $c(f)$ is a unit). Note that $f = 0$ if and only if $c(f) = 0$. Note that when $f \in R[x]$ and $a \in R$ we have $c(af) = a\, c(f)$. In particular, we have $f = c(f)\, g$ for a primitive polynomial $g \in R[x]$.

11.19 Example: For $f(x) = 6x + 30 \in \mathbf{Z}[x]$ we have $c(f) = 6$. Since $\deg(f) = 1$, it follows that f is irreducible in $\mathbf{Q}[x]$. But since $c(f) = 6$, it follows that f is reducible in $\mathbf{Z}[x]$, indeed in $\mathbf{Z}[x]$ we have $f(x) = 2 \cdot 3 \cdot (x + 5)$.

11.20 Theorem: *(Gauss' Lemma) Let R be a UFD with quotient field F.*
(1) For all $f, g \in R[x]$ we have $c(fg) = c(f)c(g)$.
(2) Let $0 \neq f \in R[x]$ and let $g(x) = \frac{1}{c(f)} f(x) \in R[x]$. Then f is irreducible in $F[x]$ if and only if g is irreducible in $R[x]$.
(3) Let $0 \neq f \in R[x]$. Then f is reducible in $F[x]$ if and only if f can be factored as a product of two nonconstant polynomials in $R[x]$.

Proof: Let $f, g \in R[x]$. If $f = 0$ or $g = 0$ then we have $c(fg) = 0 = c(f)c(g)$. Suppose that $f \neq 0$ and $g \neq 0$. Let $h(x) = \frac{1}{c(f)} f(x)$ and $k(x) = \frac{1}{c(g)} g(x)$. Then we have $h, k \in R[x]$ with $c(h) = c(k) = 1$ and $fg = c(f)c(g)hk$ so that $c(fg) = c(f)c(g)c(hk)$. Thus to prove Part (1) it suffices to show that $c(hk) = 1$. Let $h(x) = \sum_{i=0}^{n} a_i x^i$ and $k(x) = \sum_{i=0}^{m} b_i x^i$ with $a_n \neq 0$ and $b_m \neq 0$. Suppose, for a contradiction, that $c(hk) \neq 1$. Let p be a prime factor of $c(hk)$. Then p divides all of the coefficients of $(hk)(x) = (a_0 b_0) + (a_1 b_0 + a_0 b_1)x + \cdots + (a_n b_m)x^{n+m}$. Since $c(h) = 1$, p does not divide all the coefficients of $h(x)$, so we can choose an index $r \geq 0$ so that $p | a_i$ for all $i < r$ and $p \not| a_r$. Since $c(k) = 1$ we can choose an index $s \geq 0$ so that $p | b_i$ for all $i < s$ and $p \not| b_s$. Since p divides every coefficient of $(hk)(x)$, it follows that in particular p divides the coefficient

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_r b_s + \cdots + a_{r+s-1} b_1 + a_{r+s}.$$

Since $p | c_{r+s}$ and $p | a_i$ for all $i < r$ and $p | b_i$ for all $i < s$ it follows that $p | a_r b_s$. Since p is prime and $p | a_r b_s$ it follows that $p | a_r$ or $p | b_s$. But r and s were chosen so that $p \not| a_r$ and $p \not| b_s$ so we have obtained the desired contradiction. This proves Part (1).

To prove Parts (2) and (3), let $0 \neq f(x) \in R[x]$ and let $g(x) = \frac{1}{c(f)} f(x)$, and note that $g \in R[x]$ with $c(g) = 1$. Suppose that g is reducible in $R[x]$, say $g(x) = h(x)k(x)$ where $h(x)$ and $k(x)$ are non-units in $R[x]$. Since $c(h)c(k) = c(hk) = c(g) = 1$ it follows that $c(h) = c(k) = 1$. Note that $h(x)$ cannot be a constant polynomial since if we had $h(x) = r$ with $r \in R$, then we would have $c(h) = r$ and also $c(h) = 1$ so that r is a unit in R, but then h would be a unit in $R[x]$. Similarly $k(x)$ cannot be a constant polynomial. Since $h(x)$ and

$k(x)$ are nonconstant polynomials in $R[x]$, they are also nonconstant polynomials in $F[x]$. Since $f(x) = c(f)g(x) = c(f)h(x)k(x)$ and since $c(f)h(x)$ and $k(x)$ are both nonconstant polynomials (hence nonunits) in $F[x]$, it follows that $f(x)$ is reducible in $F[x]$.

Conversely, suppose that $f(x)$ is reducible in $F[x]$, say $f(x) = h(x)k(x)$ where h and k are nonzero, nonunits in $F[x]$. Since h and k are nonzero nonunits in $F[x]$, they are nonconstant polynomials. Let a be a least common multiple of the denominators of the coefficients of $h(x)$ and let b be a least common multiple of denominators of the coefficients of $k(x)$, and note that $ah(x) \in R[x]$ and $bk(x) \in R[x]$. Let $p(x) = \frac{1}{c(ah)}ah(x)$ and let $q(x) = \frac{1}{c(bk)}bk(x)$ and note that $p(x), q(x) \in R[x]$ with $c(p) = c(q) = 1$ and that $\deg(p) = \deg(h)$ and $\deg(q) = \deg(k)$. Since $f(x) = ah(x)\,bk(x) = c(ah)c(bk)p(x)q(x)$ we have $c(f) = c(ah)c(bk)c(pq) = c(ah)c(bk)$ so $g(x) = \frac{1}{c(f)}f(x) = \frac{1}{c(ah)c(bk)}ah(x)\,bk(x) = p(x)q(x)$. Since $g(x) = p(x)q(x)$ where $p(x)$ and $q(x)$ are nonconstant polynomials in $R[x]$, we see that $g(x)$ is reducible in $R[x]$.

11.21 Theorem: (*Modular Reduction*) *Let* $f(x) = \sum_{i=0}^{n} c_i x^i$ *with* $n \in \mathbf{Z}^+$, $c_i \in \mathbf{Z}$ *and* $c_n \neq 0$. *Let* p *be a prime number with* $p \nmid c_n$. *Let* $\overline{f}(x) = \sum_{i=0}^{n} \overline{c_i}\, x^i \in \mathbf{Z}_p[x]$ *where* $\overline{c_i} = [c_i] \in \mathbf{Z}_p$. *If* $\overline{f}$ *is irreducible in* $\mathbf{Z}_p[x]$ *then* f *is irreducible in* $\mathbf{Q}[x]$.

Proof: Suppose that $f(x)$ is reducible in $\mathbf{Q}[x]$. By Gauss' Lemma, we can choose two nonconstant polynomials $g, h \in \mathbf{Z}[x]$ such that $f = gh \in \mathbf{Z}[x]$. Write $g(x) = \sum_{i=0}^{k} a_i x^k \in \mathbf{Z}[x]$ and $h(x) = \sum_{i=0}^{\ell} b_i x^i \in \mathbf{Z}[x]$ with $a_k \neq 0$, $b_\ell \neq 0$ and $k, \ell \geq 1$. Let $\overline{g} = \sum_{i=0}^{k} \overline{a}_i x^i \in \mathbf{Z}_p[x]$ and $\overline{h}(x) = \sum_{i=0}^{\ell} \overline{b}_i x^i \in \mathbf{Z}_p[x]$, and note that $\overline{f} = \overline{g}\,\overline{h} \in \mathbf{Z}_p[x]$. Since $c_n = a_k b_\ell$ and $p \nmid c_n$ it follows that $p \nmid a_k$ and $p \nmid b_\ell$ in $\mathbf{Z}$ so $\overline{a}_k \neq 0$ and $\overline{b}_\ell \neq 0$ in $\mathbf{Z}_p$. Thus $\deg(\overline{g}) = \deg(g) = k$ and $\deg(\overline{h}) = \deg(h) = \ell$ so that $\overline{g}$ and $\overline{h}$ are nonconstant polynomials in $\mathbf{Z}_p[x]$, and so the polynomial $\overline{f} = \overline{g}\overline{h}$ is reducible in $\mathbf{Z}_p[x]$.

11.22 Example: Prove that $f(x) = x^5 + 2x + 4$ is irreducible in $\mathbf{Q}[x]$ by working in $\mathbf{Z}_3[x]$.

11.23 Theorem: (*Eisenstein's Criterion*) *Let* $f(x) = \sum_{i=0}^{n} c_i x^i$ *with* $n \in \mathbf{Z}^+$, $c_i \in \mathbf{Z}$ *and* $c_n \neq 0$. *Let* p *be a prime number such that* $p_i | c_i$ *for* $0 \leq i < n$ *and* $p \nmid c_n$ *and* $p^2 \nmid c_0$. *Then* f *is irreducible in* $\mathbf{Q}[x]$.

Proof: Suppose, for a contradiction, that $f(x)$ is reducible in $\mathbf{Q}[x]$. By Gauss' Lemma, we can choose two nonconstant polynomials $g, h \in \mathbf{Z}[x]$ such that $f = gh \in \mathbf{Z}[x]$. Write $g(x) = \sum_{i=0}^{k} a_i x^k \in \mathbf{Z}[x]$ and $h(x) = \sum_{i=0}^{\ell} b_i x^i \in \mathbf{Z}[x]$ with $k, \ell \geq 1$ and $a_k \neq 0$, $b_\ell \neq 0$. Since $c_0 = a_0 b_0$ and $p | c_0$ but $p^2 \nmid c_0$, it follows that p divides exactly one of the two numbers a_0 and b_0. Suppose that p divides a_0 but not b_0 (the case that p divides b_0 but not a_0 is similar). Since $p | c_1$, that is $p \big| (a_0 b_1 + a_1 b_0)$, and $p | a_0$ it follows that $p | a_1 b_0$, and since $p \nmid b_0$ it follows that $p | a_1$. Since $p | c_2$, that is $p \big| (a_0 b_2 + a_1 b_1 + a_2 b_0)$ and $p | a_0$ and $p | a_1$, it follows that $p | a_2 b_0$, and since $p \nmid b_0$ it then follows that $p | a_2$. Repeating this argument we find, inductively, that $p | a_i$ for all $i \geq 0$, and in particular we have $p | a_k$. Since $c_n = a_k b_\ell$ and $p | a_k$ it follows that $p | c_n$, giving the desired contradiction.

11.24 Example: Note that $f(x) = 5x^5 + 3x^4 - 18x^3 + 12x + 6$ is irreducible in $\mathbf{Q}[x]$ by Eisenstein's Criterion using $p = 3$.

11.25 Example: Let p be a prime number. Show that $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible in $\mathbf{Q}[x]$,

11.26 Theorem: *If R is a UFD then so is $R[x]$.*

Proof: Suppose that R is a UFD and let F be the quotient field of R. Note that the units in $R[x]$ are the constant polynomials which are also units in R. Let $f \in R[x]$ be a non-zero non-unit. If f is a constant polynomial, then the factorization of f in $R[x]$ is the same as the factorization of f in R. Suppose that $\deg(f) \geq 1$. Let $g = \frac{1}{c(f)} f$ so that $g \in R[x]$ with $c(g) = 1$. The factorization of $c(f)$ in $R[x]$ is the same as the factorization in R, so it suffices to show that the polynomial g factors uniquely into irreducibles in $R[x]$. Since $F[x]$ is a ED, hence a UFD, we know that g factors into irreducibles in $F[x]$. By Gauss' Lemma, we can multiply each of the irreducible factors in $F[x]$ by an element of F to write g as a product of irreducible factors in $R[x]$, say $g = f_1 f_2 \cdots f_\ell$ where each f_j is irreducible in $R[x]$. Since $c(g) = 1$ we must have $c(f_j) = 1$ for each index j.

Suppose that $g = f_1 f_2 \cdots f_\ell = g_1 g_2 \cdots g_m$ where f_j and g_k are irreducible in $R[x]$ with $c(f_j) = c(g_k) = 1$ for all j, k. Note that each f_j must be non-constant since if we had $f_j(x) = r \in R$ then we would have $c(f_j) = r$ and $c(f_j) = 1$ so that r is a unit in R, but then f_j would be a unit in $R[x]$. Similarly each g_k is non-constant. It follows that the polynomials f_j and g_k are also irreducible in $F[x]$. By unique factorization in $F[x]$, we must have $m = \ell$ and, after possibly reordering the polynomials g_k, we have $f_j \sim g_j$ in $F[x]$ for all indices j. Since $f_j \sim g_j$ in $F[x]$, we have $g_j = u f_j$ for some $0 \neq u \in F$. Say $u = \frac{a}{b}$ where $a, b \in R$ with $\gcd(a, b) = 1$. Then we have $a\, f_j = b\, g_j$ in $R[x]$. Since $c(f_j) = c(g_j) = 1$ we have $c(af_j) = a$ and $c(bg_j) = b$ and it follows that $a \sim b$ in R, hence $a = bv$ for some unit $v \in R$. Thus we have $g_j = u f_j = \frac{a}{b} f_j = v f_j$ and so $f_j \sim g_j$ in $R[x]$.

11.27 Corollary: *If R is a UFD then so is the polynomial ring $R[x_1, x_2, \cdots, x_n]$.*

.