Chapter 1. Definitions and Examples of Groups

1.1 Definition: For a set S we write $S \times S = \{(a,b)|a \in S, b \in S\}$. A **binary operation** on S is a map $* : S \times S \to S$, where for $a, b \in S$ we usually write $*(a,b)$ as $a * b$.

1.2 Definition: A **ring** (with identity) is a set R together with two binary operations $+$ and $\cdot$ (called **addition** and **multiplication**), where for $a, b \in R$ we often write $a \cdot b$ as ab, and two distinct elements $0, 1 \in R$ (called the **zero** and the **identity** elements), 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 $a, b \in R$,
(3) 0 is an additive identity: $0 + a = a$ for all $a \in R$,
(4) every element has an additive inverse: for every $a \in R$ there exists $b \in R$ with $a+b = 0$,
(5) $\cdot$ is associative: $(ab)c = a(bc)$ for all $a, b, c \in R$,
(6) 1 is a multiplicative identity: $1 \cdot a = a = a \cdot 1$ for all $a \in R$, and
(7) $\cdot$ is distributive over $+$: $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all $a, b, c \in R$,

A ring R is called **commutative** when
(8) $\cdot$ is commutative: $ab = ba$ for all $a, b \in R$.

For $0 \neq a \in R$, we say that a is a **unit** (or that a is **invertible**) when there exists an element $b \in R$ such that $ab = 1 = ba$. A **field** is a commutative ring R such that
(9) every non-zero element is a unit: for every $0 \neq a \in R$ there exists $b \in R$ with $ab = 1$.

1.3 Example: The set of **integers** $\mathbb{Z}$ is a commutative ring, but it is not a field because it does not satisfy Property (9). The set of **positive integers** $\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$ is not a ring because $0 \notin \mathbb{Z}^+$ and $\mathbb{Z}^+$ does not satisfy Properties (3) and (4). The set of **natural numbers** $\mathbb{N} = \{0, 1, 2, \cdots\}$ is not a ring because it does not satisfy Property (4). The set of **rational numbers** $\mathbb{Q}$, the set of **real numbers** $\mathbb{R}$ and the set of **complex numbers** $\mathbb{C}$ are all fields. For $2 \leq n \in \mathbb{Z}$, the set $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ of **integers modulo** n is a commutative ring, and $\mathbb{Z}_n$ is a field if and only if n is prime (in $\mathbb{Z}_1 = \{0\}$ we have $0 = 1$, so $\mathbb{Z}_1$ is not a ring with identity).

1.4 Example: Given a ring R, the set $R[x]$ of **polynomials** with coefficients in R is a ring (under the usual addition and multiplication of polynomials). If R is commutative then so is $R[x]$.

1.5 Example: Given a ring R and a positive integer n, the set $M_n(R)$ of $n \times n$ **matrices** with entries in R is a ring (under matrix addition and matrix multiplication). When $n \geq 2$, the ring $M_n(R)$ is not commutative.

1.6 Example: Given rings R and S, the **product** $R \times S = \big\{(a,b)\big|a \in R, b \in S\big\}$ is a ring (under componentwise addition and multiplication). If R and S are both commutative then so is $R \times S$. More generally, given a positive integer n and given rings $R_1, R_2, \cdots, R_n$, the **product** $\prod\limits_{i=1}^{n} R_i = R_1 \times R_2 \times \cdots \times R_n = \big\{(a_1, a_2, \cdots, a_n)\big|a_i \in R_i\big\}$ is a ring (under componentwise addition and multiplication). Given a ring R and a positive integer n we write $R^n = \prod\limits_{i=1}^{n} R = R \times R \times \cdots \cdots R$.

1.7 Theorem: (*Uniqueness of the Inverse*) *Let R be a ring. Let $a \in R$. Then*
(1) the additive inverse of a is unique: if $a+b=0=a+c$ then $b=c$,
(2) if a has an inverse then it is unique: if $ab=1=ba$ and $ac=1=ca$ then $b=c$.

Proof: To prove (1), suppose that $a+b=0=a+c$. Then

$$b=0+b=(a+c)+b=b+(a+c)=(b+a)+c=(a+b)+c=0+c=c\,.$$

To prove (2), suppose that $ab=1=ba$ and $ac=1=ca$. Then

$$b=1\cdot b=(ca)b=c(ab)=c\cdot 1=c\,.$$

1.8 Definition: Let R be a ring and let $a,b\in R$. We write the (unique) additive inverse of a as $-a$, and we write $b-a=b+(-a)$. If $a\neq 0$ has a multiplicative inverse, we write the (unique) multiplicative inverse of a as a^{-1}. When R is commutative we also write a^{-1} as $\frac{1}{a}$, and we write $\frac{b}{a}=b\cdot\frac{1}{a}$.

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

Let F be a field. Then for all $a,b,c\in F$ we have
(4) if $ab=ac$ then either $a=0$ or $b=c$.
(5) if $ab=a$ then either $a=0$ or $b=1$,
(6) if $ab=1$ then $b=a^{-1}$, and
(7) if $ab=0$ then either $a=0$ or $b=0$.

Proof: To prove (1), suppose that $a+b=a+c$. Then we have

$$b=0+b=-a+a+b=-a+a+c=0+c=c\,.$$

Part (2) follows from part (1) since if $a+b=a$ then $a+b=a+0$, and part (3) follows from part (1) since if $a+b=0$ then $a+b=a+(-a)$. To prove part (4), suppose that $ab=ac$ and $a\neq 0$. Then we have

$$b=1\cdot b=a^{-1}ab=a^{-1}ac=1\cdot c=c\,.$$

Note that parts (5), (6) and (7) all follow from part (4).

1.10 Remark: In the above proof, we used associativity and commutativity implicitly. If we wished to be explicit then the proof of part (1) would be as follows. Suppose that $a+b=a+c$. Then we have

$$b=0+b=(a-a)+b=(-a+a)+b=-a+(a+b)=-a+(a+c)=(-a+a)+c=0+c=c.$$

In the future, we shall often use associativity and commutativity implicitly in our calculations.

1.11 Theorem: (*Multiplication by 0 and -1*) *Let R be a ring and let $a\in R$. Then*
(1) $0\cdot a=0$, and
(2) $(-1)a=-a$.

Proof: We have $0a=(0+0)a=0a+0a$. Subtracting $0a$ from both sides (using part 1 of the Cancellation Theorem) gives $0=0a$. Also, we have $a+(-1)a=(1)a+(-1)a=(1+(-1))a=0a=0$, and subtracting a from both sides gives $(-1)a=-a$.

1.12 Definition: A **group** is a set G together with a binary operation $*: G \times G \to G$ 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 $a*b = b*a = e$.

A group G is called **abelian** when

(4) $*$ is commutative: $a*b = b*a$ for all $a,b \in G$.

1.13 Example: If R is a ring under the operations $+$ and $\cdot$, then R is also an abelian group under $+$ with identity 0. For example, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_n$ are abelian groups under $+$ with identity 0.

1.14 Example: If R is a ring under $\cdot$ with identity 1 then the set of units

$$R^* = \left\{a \in R \,\middle|\, a \text{ is invertible}\right\}$$

is a group under $\cdot$ with identity 1. For example, $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ and the **group of units modulo** n

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

are all abelian groups under multiplication with identity 1.

1.15 Example: Given a ring R and a positive integer $n \in \mathbb{Z}^+$, from the ring $M_n(R)$ (under matrix addition and matrix multiplication) we obtain the abelian group $M_n(R)$ under matrix addition, and we obtain the **general linear group**

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

under matrix multiplication. The general linear group is non-abelian for $n \geq 2$.

1.16 Example: If G and H are groups with identities e and u, then the **product**

$$G \times H = \left\{(a,b) \,\middle|\, a \in G, b \in H\right\}$$

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

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

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 $G^n = \prod_{i=1}^{n} G = G \times G \times \cdots \times G$.

1.17 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 $n \in \mathbb{Z}^+$, the n^{th} **symmetric group** is the group

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

1.18 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 $u = u * v = v$.

1.19 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

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

1.20 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 element $a \in G$ by $-a$. For $a, b \in G$, we write $a - b = a + (-b)$. For $a \in G$ and $k \in \mathbb{Z}^+$ 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 $k, l \in \mathbb{Z}$ we have $(k + l)a = ka + la$, $(-k)a = -(ka) = k(-a)$, $-(-a) = a$ and $-(a + b) = -a - b = -b - a$.

1.21 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 $k \in \mathbb{Z}^+$ 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 $k, l \in \mathbb{Z}$ we have $a^{k+l} = a^k a^l$, $a^{-k} = (a^k)^{-1} = (a^{-1})^k$, $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.

1.22 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 $ab = a$ then $b = e$ and if $ab = b$ then $a = e$.

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 $ab = b$ then multiplying on the right by b^{-1} gives $a = e$.

1.23 Definition: For a finite group G (that is a group which has finitely many elements), 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.

1.24 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

1.25 Definition: Let G be a group and let $a \in G$. The **order** of G is its cardinality $|G|$ (when G is finite, the cardinality $|G|$ is the number of elements in G). The **order** of a in G, denoted by $|a|$ or by $\mathrm{ord}_G(a)$, 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.

1.26 Example: In any group G, the order of the identity element is $|e| = 1$.

1.27 Example: The order of the group $\mathbb{Z}$ is $|\mathbb{Z}| = \infty$ (or more accurately, $|\mathbb{Z}| = \aleph_0$). In $\mathbb{Z}$ we have $|0| = 1$ and for $0 \neq a \in \mathbb{Z}$ we have $|a| = \infty$ (because $na \neq 0$ for all $n \in \mathbb{Z}^+$).

1.28 Example: The order of $\mathbb{Z}_n$ is $\big|\mathbb{Z}_n\big| = n$. The order of $a \in \mathbb{Z}_n$ 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 $ka = 0 \in \mathbb{Z}_n \iff n|ka \iff td|ksd \iff t|ks \iff t|k$ and so $|a| = t = \frac{n}{d}$.

1.29 Example: The order of U_n is $|U_n| = \varphi(n)$ where $\varphi(n)$ is the Euler phi number of n. We shall see later (in Corollary 4.22) that if $n = \prod {p_i}^{k_i}$ is the prime factorization of n then $\varphi(n) = \prod ({p_i}^{k_i} - {p_i}^{k_i - 1})$.

1.30 Example: The order of the group $\mathbb{C}^*$ is $|\mathbb{C}^*| = \infty$ (or more accurately $|\mathbb{C}^*| = 2^{\aleph_0}$). For $a = re^{i\,\theta} \in \mathbb{C}^*$ where $r, \theta \in \mathbb{R}$ 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 $k, n \in \mathbb{Z}$ and $n \neq 0$ we have $|a| = \frac{n}{\gcd(k,n)}$.

1.31 Example: If S is a finite set then $\big|\mathrm{Perm}(S)\big| = |S|!$ and in particular $|S_n| = n!$.

1.32 Example: When p is prime (so that $\mathbb{Z}_p$ is a field), we have

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

Indeed, for a matrix $A \in M_n(\mathbb{Z}_p)$, 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 ${\mathbb{Z}_p}^n$ so there are $p^n - 1$ choices for u_1. Having chosen u_1, the second column u_2 can be any vector in ${\mathbb{Z}_p}^n$ which is not a multiple $t_1 u_1$, $t_1 \in \mathbb{Z}_p$. 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 ${\mathbb{Z}_p}^n$ which is not a linear combination $t_1 u_1 + t_2 u_2$, $t_1, t_2 \in \mathbb{Z}_p$. There are p^2 such linear combinations, so there are $p^n - p^2$ choices for u_3. And so on.

1.33 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

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

1.34 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.

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