

# MATH322, modern algebra

Samuel Lindskog

December 11, 2024

## 1 Background

**Definition 1.1** (Relation). Suppose  $A$  and  $B$  are sets. A subset  $R \subseteq A \times B$  is a relation from  $A$  to  $B$ .

**Definition 1.2.** Suppose  $R$  a relation on  $A$ . Then:

1.  $R$  is reflexive on  $A$  if  $\forall x \in A, xRx$
2.  $R$  is symmetric on  $A$  if  $\forall a, b \in A, aRb \Rightarrow bRa$
3.  $R$  is antisymmetric on  $A$  if  $\forall a, b \in A, aRb \wedge bRa \Rightarrow a = b$
4.  $R$  is transitive on  $A$  if  $\forall a, b, c \in A, aRb \wedge bRc \Rightarrow aRc$

**Definition 1.3** (Equivalence relation). Suppose  $R$  a relation on  $A$ .  $R$  is an equivalence relation if  $R$  is reflexive, symmetric, and transitive.

**Definition 1.4** (Well ordering of  $\mathbb{Z}$ ). If  $A$  is any nonempty subset of  $\mathbb{Z}^+$ ,

$$\exists m \in A \forall a \in A, m \leq a$$

**Definition 1.5** (Divisibility). If  $a, b \in \mathbb{Z}$  with  $a \neq 0$ , we say  $a$  divides  $b$  (denoted  $a|b$ ) if there is an element  $c \in \mathbb{Z}$  such that  $b = ac$ .

**Definition 1.6** (GCD). If  $a, b \in \mathbb{Z} \setminus \{0\}$ , there is a unique positive integer  $d$ , called the greatest common divisor of  $a$  and  $b$ , satisfying:

1.  $d|a$  and  $d|b$
2. if  $e|a$  and  $e|b$ , then  $e|d$

If the GCD of  $a$  and  $b$  is 1, then we say  $a$  and  $b$  are relatively prime.

**Definition 1.7** (LCM). If  $a, b \in \mathbb{Z} \setminus \{0\}$ , there is a unique positive integer  $l$  called the least common multiple of  $a$  and  $b$  satisfying:

1.  $a|l$  and  $b|l$
2. if  $a|m$  and  $b|m$ , then  $l|m$

*Remark.* The relationship between the GCD  $d$  and the LCM  $l$  is  $dl = ab$ . For intuition, think of  $a$  and  $b$  separated into their prime factors, LCM by necessity is the product of the union of prime factors from  $a$  and  $b$ . The product of intersection of prime factors is the GCD.

**Definition 1.8** (Division algorithm). If  $a, b \in \mathbb{Z} \setminus \{0\}$ , then there exist unique  $q, r \in \mathbb{Z}$  such that

$$a = qb + r \text{ and } 0 \leq r < |b|,$$

where  $q$  is the quotient and  $r$  the remainder.

**Lemma 1.1.** If  $a, b \in \mathbb{Z} \setminus \{0\}$  and using the division algorithm

$$a = qb + r,$$

it follows that if  $r > 0$ , the GCD of  $b$  and  $r$  is equal to the GCD of  $a$  and  $b$ . If  $r = 0$ , the GCD of  $a$  and  $b$  is  $b$ .

*Proof:* In the case that  $r > 0$ , suppose  $g_{ab}$  is the GCD of  $a$  and  $b$ , and that  $g_{br}$  is the GCD of  $b$  and  $r$ .  $g_{ab}|b$  and  $g_{ab}|qb + r$  so  $g_{ab}|r$ . Thus  $g_{ab}|g_{br}$  and  $g_{ab} \leq g_{br}$ . Clearly  $g_{br}|qb + r$  so  $g_{br}|a$  and  $g_{br}|g_{ab}$  so  $g_{ab} \geq g_{br}$ . Therefore  $g_{br} = g_{ab}$ .

In the case that  $r = 0$ ,  $b|qb$  so  $b|a$  and  $b|b$ . Clearly condition two of the definition of GCD is satisfied by  $b$ , so  $b$  is the *GCD* of  $a$  and  $b$ .  $\square$

**Definition 1.9** (Euclidean algorithm). This procedure produces a GCD of two integers  $a$  and  $b$  by iterating the division algorithm. If  $a, b \in \mathbb{Z} \setminus \{0\}$ , inductively define the sequence  $\{r_n\}_{n=0}^k$  as follows:

$$\begin{cases} n = 0, & r_0 = b \\ n = 1, r_1 > 0 & ? \quad a = q_1 r_0 + r_1 \quad : \quad k = n - 1 \quad \# \text{ return} \\ n > 1, r_{n-1} > 0 & ? \quad r_{n-2} = q_n r_{n-1} + r_n \quad : \quad k = n - 1 \end{cases}$$

The last element in the sequence is the GCD of  $a$  and  $b$ .

*Proof:* Following lemma 1.1, the last element of  $r_k$  of  $\{r_n\}$  is the GCD of its pair  $r_{k-1}, r_k$  because  $r_{k+1} = 0$ , and thus is the GCD of each preceding pair in the sequence.  $\square$

**Definition 1.10** (Partition). Suppose  $A$  is a set and  $\mathcal{F} \subseteq \mathcal{P}(A)$ .  $\mathcal{F}$  is called a partition of  $A$  if it has the following properties:

1.  $\bigcup \mathcal{F} = A$
2.  $\mathcal{F}$  is pairwise disjoint.
3.  $\forall X \in \mathcal{F}, X \neq \emptyset$

## 2 Binary operators, groups and subgroups

**Definition 2.1** (Binary operation). A binary operation  $*$  on a set  $S$  is a function

$$* : (S \times S) \rightarrow S$$

**Definition 2.2** (Group). A group  $(G, \cdot)$  is a set  $G$  with the operation  $\cdot$  defined

$$\cdot : G \times G \rightarrow G$$

that satisfies the following properties:

1.  $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ . (associativity)
2.  $\exists e \in G \forall a \in G, e \cdot a = a = a \cdot e$ . (identity element)
3.  $\forall a \exists a', a' \cdot a = e = a \cdot a'$ . (inverse element)

Commutativity of the inverse and identity elements is a consequence of

**Theorem 2.1** (Identity of a group is unique).

*Proof:* Suppose  $e$  and  $\bar{e}$  identity elements of a group. Then

$$e \cdot \bar{e} = e = \bar{e}.$$

$\square$

**Lemma 2.1.** If  $(G, \cdot)$  is a group, then for all  $a, b, c \in G$ ,

$$\begin{aligned} a \cdot b = a \cdot c &\Rightarrow b = c, \\ b \cdot a = c \cdot a &\Rightarrow b = c, \end{aligned}$$

*Proof:* This proof utilizes all three group axioms, and shows group elements are duck-typed. First we prove left cancellation. Suppose  $a \cdot b = a \cdot c$ . Then

$$\begin{aligned} a' \cdot (a \cdot b) &= a' \cdot (a \cdot c) \\ (a' \cdot a) \cdot b &= (a' \cdot a) \cdot c \\ e \cdot b &= e \cdot c \\ b &= c \end{aligned}$$

Next, we prove right cancellation. Suppose  $b \cdot a = c \cdot a$ . Then

$$\begin{aligned}(b \cdot a) \cdot a' &= (c \cdot a) \cdot a' \\ b \cdot (a \cdot a') &= c \cdot (a \cdot a') \\ b \cdot e &= c \cdot e \\ b &= c\end{aligned}$$

□

**Corollary 2.1.** For elements  $a, c \in (G, \cdot)$  the element  $b \in G$  such that  $a \cdot b = c$ , is unique.

**Definition 2.3** (Abelian). An abelian group is one for which its group operator is commutative.

*Remark* (Multiplicative and additive groups). The use of  $+$  or  $\cdot$  as the group operator is notational preference, however additive groups usually refer to an abelian group. By default, when we say that  $G$  is a group, we mean that  $(G, \cdot)$  is a multiplicative group, and utilize notation accordingly.

**Definition 2.4** (Subgroup). We say that  $H$  is a subgroup of  $G$ , denoted  $H \leq G$ , if  $G, H$  are groups with the same group operation and  $G \subseteq H$ .

**Theorem 2.2** (Subgroup test). Let  $G$  be a group. Then  $H \leq G$  iff

1.  $\emptyset \neq H \subseteq G$
2.  $a, b \in H \Rightarrow ab^{-1} \in H$

*Proof:* We must prove that the  $\cdot$  operation on  $H$  is defined on  $H \times H$ , and that group axioms hold on  $H$ . Suppose  $G$  a group, and  $H$  meets the above criteria. If  $a \in H$  then  $aa^{-1} = e \in H$ . It follows that  $ea^{-1} = a^{-1} \in H$ , and thus every element in  $H$  has an inverse in  $H$ . Therefore for any  $b, c \in H$ ,  $c^{-1} \in H$  and  $bc \in H$  so  $H$  is closed under the group operation on  $G$ . The group operation on  $H$  is associative by definition, so  $H$  is a subgroup. The right implication is trivial. □

**Definition 2.5** (Modulo and equivalence classes). If  $a, b \in \mathbb{Z}$ ,  $a$  modulo  $b$ , denoted  $a \bmod b$  is the remainder of  $a|b$ . Suppose  $\sim$  is an equivalence relation on a set  $A$ , and  $x \in A$ . Then the *equivalence class* of  $x$  with respect to  $\sim$  is the set

$$[x] = \{y \in A \mid y \sim x\}.$$

The set of all equivalence classes of elements  $A$  is called  $A$  modulo  $\sim$  and denoted  $A/\sim$ . The equivalence class mod  $n$  of  $a$  is the set of all integers which differ from  $a$  by some integer multiple of  $n$ . The integers modulo  $n$ , denoted  $\mathbb{Z}/n\mathbb{Z}$ , is the set of equivalence classes mod  $n$  of all integers.

**Theorem 2.3.** Suppose  $\sim$  is an equivalence relation on  $A \neq \emptyset$ . Then  $A/\sim$  is a partition of  $A$ .

*Proof:*  $A/\sim$  contains  $[x]$  for each  $x \in A$ . Because  $\sim$  is reflexive,  $x \in [x]$ , so  $A \subseteq \bigcup A/\sim$ . Because  $\sim$  a relation on  $A$ ,  $\bigcup A/\sim \subseteq A$ , and thus  $\bigcup A/\sim = A$ . Suppose  $[a], [b] \in A/\sim$ , and suppose to the contrary there exists  $c \in A$  such that  $c \in [a] \cap [b]$ . Because  $aRc$  and  $cRb$  we have  $aRb$ . Then if  $x \in [a]$  and  $y \in [b]$  we have  $xRa$  and  $bRy$ , so  $xRy$  and thus  $[a] = [b]$ , a contradiction. Therefore  $[a] \cap [b] = \emptyset$ . Each  $[a] \in A$  contains  $a \in A$  because  $\sim$  reflexive, so  $[a] \neq \emptyset$ . □

### 3 Cosets, normal subgroups, cyclic groups

**Definition 3.1.** Let  $H \leq G$ . Define the relation  $\sim$  on  $G$  by  $a \sim b$  if  $b^{-1}a \in H$ .

*Remark.* For the remainder of discussion of groups within these notes,  $\sim$  represents the above relation.

**Theorem 3.1.**  $\sim$  is an equivalence relation on  $G$ .

*Proof:*

1. For any  $a \in G$ ,  $a^{-1}a = e \in H$ , so  $\sim$  is reflexive.
2. Suppose  $a, b \in G$  and  $a \sim b$ . Then  $b^{-1}a \in H$ , so  $a^{-1}b \in H$  and  $\sim$  is symmetric.
3. Suppose  $a, b, c \in G$  and  $a \sim b$  as well as  $b \sim c$ . Then

$$\begin{aligned} b^{-1}a &\in H \wedge c^{-1}b \in H \\ a^{-1}b &\in H \wedge b^{-1}c \in H \\ a^{-1}c &\in H \\ c^{-1}a &\in H \\ \Rightarrow aRc \end{aligned}$$

so  $\sim$  is transitive. □

**Lemma 3.1.** If  $a \notin H$ , then  $e \notin [a]$

*Proof:* If  $e \in [a]$ , then  $a^{-1}e \in H$  and thus  $a \in H$ . □

**Lemma 3.2.**  $a \in H$  and  $b \in [a]$  iff  $b \in H$ .

*Proof:* Following lemma 3.1,  $eRa$ . Because  $\sim$  is transitive and symmetric,

$$bRa \Rightarrow aRb \Rightarrow eRb \Rightarrow b^{-1}e \in H \Rightarrow b \in H.$$

If  $a, b \in H$ ,  $ab \in H$ . □

**Definition 3.2** (Left coset). Let  $H \leq G$  and  $a \in G$ . We say that

$$aH = \{ah \mid h \in H\} = [a]$$

is the left coset of  $H$  containing  $a$ .

*Remark.* For additive groups, we would write the left coset of  $H$  containing  $a$  as

$$a + H.$$

*Remark.* Let  $H \leq G$ . Set

$$G//H = \{aH \mid a \in G\}$$

**Theorem 3.2** (Lagrange's theorem). Let  $|G| < \infty$  and  $H \leq G$ . Then  $|H|$  divides  $|G|$ .

*Proof:* We know from lemma 3.6 that for all  $a$ ,  $|aH| = |H|$ . Following lemma 2.3,  $G//H$  is a partition of  $G$ , so  $|G| = |G//H| |H|$ . □

**Definition 3.3** (Index). Let  $H \leq G$ . Define the index  $[G : H]$  of  $H$  in  $G$  by

$$[G : H] = |G//H|$$

*Remark.* Lagrange's theorem implies that

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

**Definition 3.4.** Let  $H \leq G$ . We say that  $H$  is a normal subgroup of  $G$ , written  $H \trianglelefteq G$ , if  $aH = Ha$  for all  $a \in G$ .

**Lemma 3.3.** Let  $H \leq G$ . Then  $H \trianglelefteq G$  iff  $aHa^{-1} = H$  for all  $a \in G$ .

**Lemma 3.4.** If  $G$  is an abelian group and  $H \leq G$ , then  $H \trianglelefteq G$ .

*Proof:* Because  $G$  is abelian,

$$aH = \{ah \mid h \in H\} = \{ha \mid h \in G\} = Ha.$$

□

**Theorem 3.3.** Let  $H \leq G$ . Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

iff  $H \trianglelefteq G$ .

*Proof:* To prove the right implication, suppose  $aHbH = abH$  is well defined and  $H \leq G$ . Then for  $h_1, h_2 \in H$  and  $a, b \in G$ ,  $ah_1Hbh_2H = ah_1bh_2H = abH$ . We can then choose  $h_3, h_4 \in H$  such that

$$ah_1bh_2 = abh_3 = ab(h_4h_2)$$

It follows from lemma 3.6 that for any  $h_4$  there exists  $h_1$ , and for any  $h_1$  there exists  $h_4$ , such that the equation above is satisfied. Therefore for arbitrary  $h_1$  or arbitrary  $h_4$ ,

$$\begin{aligned} ah_1b &= abh_4 \\ h_1b &= bh_4 \end{aligned}$$

Thus  $bH \subseteq Hb$  and  $Hb \subseteq bH$ , so  $bH = Hb$  and  $H \trianglelefteq G$ . To prove the left implication, suppose  $H \trianglelefteq G$ ,  $a_1, b_1, a_2, b_2 \in G$ ,  $a_1H = a_2H$  and  $b_1H = b_2H$ . It follows that for some  $h_1, h_2, h_3 \in H$ ,

$$\begin{aligned} a_2b_2H &= a_1h_1b_1h_2H \\ &= h_3a_1b_1h_2H \\ &= h_3^{-1}h_3a_1b_1h_2h_2^{-1}H \\ &= a_1b_1H \end{aligned}$$

□

*Remark.* Let  $H \trianglelefteq G$ . Then

$$G//H = \{aH \mid a \in G\}$$

is a group under the binary operation  $(aH)(bH) = (ab)H$ . The notation  $G/H$  will be used instead of  $G//H$  from now on.

**Definition 3.5** (Homomorphism). Let  $\phi : G \rightarrow G'$  be a map of groups. We say that  $\phi$  is a group homomorphism if

$$\forall a, b \in G, \phi(ab) = \phi(a)\phi(b).$$

A group homomorphism  $\phi$  is called a group isomorphism if  $\phi$  is bijective. We then say  $G$  and  $G'$  are isomorphic, and write  $G \cong G'$ .

**Definition 3.6** (Exponentials). Let  $G$  be a group,  $a \in G$ , and  $n \in \mathbb{Z}^+$ . We define

$$a^n := a \cdot a \cdot \dots \cdot a.$$

for  $n$   $a$ 's.

**Definition 3.7** (Order). Let  $G$  be a group. Define the order of  $G$ , denoted by  $|G|$ , to be the cardinality of  $G$ .

**Definition 3.8** (Cyclic group). Let  $G$  be a group and  $a \in G$ . Then the subgroup  $\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$  of  $G$  is called the cyclic subgroup of  $G$  generated by  $a$ . In this case we say  $a$  is a generator of  $G$ .

**Lemma 3.5.** Let  $G$  be a group and  $a \in G$ . If  $a^m = 1$  for some  $m \in \mathbb{Z} \setminus \{0\}$ , then

$$\langle a \rangle = \{a^k \mid k = 0, 1, \dots, |m| - 1\}$$

*Proof:* Suppose  $b \in \langle a \rangle$ . Then  $b = a^n$  for some  $n \in \mathbb{Z}$ . Because  $n = qm + r$  for some  $q, r \in \mathbb{Z}$  with  $0 \leq r < |m|$ , and because  $a^{qm} = e^q = e$ , then  $a^n = a^{qm+r} = ea^r = a^r = b$ . Trivially  $a^r \in \langle a \rangle$ . □

**Lemma 3.6.** Let  $H \leq G$ . Then for  $a \in G$ ,  $|aH| = |H|$ .

*Proof:* By lemma 2.1, if  $h_1, h_2 \in H$  with  $ah_1 = ah_2$ , then  $h_1 = h_2$ . Therefore the function

$$\phi : aH \rightarrow H, \quad ah \rightarrow h$$

is injective.  $\phi$  is clearly surjective.  $\square$

*Remark.* Let  $G$  be a group and  $a \in G$ . Then

$$|a| = \begin{cases} \min\{m \in \mathbb{Z}^+ \mid a^m = 1\} \\ \infty \end{cases}$$

**Lemma 3.7.** For  $1 \leq n \leq |a|$ ,  $a^n$  is unique.

*Proof:* Suppose  $1 \leq n, m \leq |a|$  and  $a^n = a^m$ . If  $n \neq m$ , then wlog  $n < m$ , and  $a^n = a^{n+(m-n)} = a^n a^{m-n} \Rightarrow a^{m-n} = 1$ , a contradiction.  $\square$

**Lemma 3.8.** If  $\langle a \rangle$  is finite, then  $|a| = |\langle a \rangle|$ .

*Proof:* Suppose  $|a| < |\langle a \rangle|$ . Because for any  $n \in \mathbb{Z}$ ,  $a^n = a^{n \bmod |a|}$ , it follows from the previous lemma that  $|\langle a \rangle| = |a|$ , a contradiction.  $\square$

**Corollary 3.1.** If  $|\langle a \rangle| = n$  then  $a^n = 1$ .

*Proof:* If  $|\langle a \rangle| = n$  and  $m \in \mathbb{N}$  such that  $m < n$  with  $a^m = 1$ , then for any  $l \in \mathbb{N}$ ,  $a^l = a^{qn+r} = a^r$  with  $0 \leq r < n$ , a contradiction. It follows from cancellation laws that  $a^n$  must be unique, thus  $a^n = 1$ .  $\square$

**Lemma 3.9.** Let  $G$  be a finite group and  $a \in G$ . Then  $a^{|G|} = 1$ .

*Proof:* It follows from lemma 3.8 and theorem 3.2 that  $|\langle a \rangle|$  divides  $|G|$ . Therefore if  $|a| = n$  then for some  $q \in \mathbb{N}$ ,  $a^{|G|} = a^{nq} = 1^q = 1$ .  $\square$

## 4 Direct product

**Definition 4.1.** Let  $G_1, \dots, G_n$  be groups. We use  $\prod_{i=1}^n G_i$  to denote the cartesian product  $G_1 \times \dots \times G_n$ .

**Theorem 4.1** (Direct product). Let  $G_1, \dots, G_n$  be groups. Then  $\prod_{i=1}^n G_i$  is a group under componentwise multiplication. It is called the direct product of these groups.

**Lemma 4.1.** Let  $G_1, \dots, G_n$  be groups. Then

$$\left| \prod_{i=1}^n G_i \right| = \prod_{i=1}^n |G_i|.$$

*Proof:* This follows directly from properties of the cartesian product.  $\square$

**Definition 4.2.** Let  $n \in \mathbb{Z}^+$ . Let  $Z_n = \{0, 1, \dots, n-1\}$ . Define an operation  $+_n : Z_n \times Z_n \rightarrow Z_n$  by

$$a +_n b = \begin{cases} a + b & 0 \leq a + b \leq n-1 \\ a + b - n & n \leq a + b \leq 2(n-1). \end{cases}$$

then  $Z_n$  is a group under the operation  $+_n$ . We use  $Z_n$  to denote the cyclic group of order  $n$ .

*Remark.* By theorem 3.2 we have  $Z_n \cong \mathbb{Z}/n\mathbb{Z}$ .

**Theorem 4.2** (The first group isomorphism theorem). Let  $\phi : G \rightarrow G'$  be a group homomorphism with

$$\text{Ker}(\phi) := \phi^{-1}(1') = \{a \in G \mid \phi(a) = 1'\}.$$

Then we have a natural group isomorphism

$$\begin{aligned} \mu : G/\text{Ker}(\phi) &\rightarrow \phi(G) \\ [a] &\rightarrow \phi(a). \end{aligned}$$

## 5 Permutations and dihedral groups

**Definition 5.1** (Permutation). A permutation of  $A$  is a bijective function  $\phi : A \rightarrow A$ . Define the set  $S_A$  by

$$S_A := \{\sigma \mid \sigma \text{ is a permutation of } A\}.$$

*Remark.*  $(S_A, \circ)$  is a group.

**Definition 5.2** (Symmetric group).  $S_A$  is called the symmetric group on  $A$ . In particular, when  $n \in \mathbb{Z}^+$  and  $A = \{1, \dots, n\}$ , the symmetric group on  $A$  is denoted  $S_n$ , and is called the symmetric group of degree  $n$ .

**Lemma 5.1.** Let  $G$  be a group of  $|G| = p$ , where  $p$  is prime. Then  $G \cong Z_p$ .

**Lemma 5.2.** If  $G$  is a group with  $|G| \leq 5$ , then  $G$  is abelian.

## 6 Group actions and counting

**Definition 6.1** (Action). Let  $X$  be a set and  $G$  be a group. An action of  $G$  on  $X$  is a function  $\cdot : G \times X \rightarrow X$  such that

1.  $\forall x \in X, 1 \cdot x = x$
2.  $\forall g_1, g_2 \in G \forall x \in X, g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x$

Under these conditions, we say that  $X$  is a  $G$ -set.

**Definition 6.2.** Let  $X$  be a  $G$ -set. We define a relation  $\sim$  on  $X$  as follows: for  $x_1, x_2 \in X$ , we say  $x_1 \sim x_2$  if there exists  $g \in G$  such that  $g \cdot x_1 = x_2$ .

*Remark.* For the remainder of the section  $\sim$  refers to the above relation when working in  $X$ .

**Theorem 6.1.** Let  $X$  be a  $G$ -set. Then  $\sim$  is an equivalence relation.

*Proof:*

1. Reflexivity: It follows from the properties of an action that  $1x = x$  for all  $x \in X$ , so  $x \sim x$ .
2. Symmetry: Suppose  $x, y \in X$  and  $x \sim y$ . Then there exists  $g \in G$  such that  $gx = y$ . But then  $g^{-1}y = x$ , so  $y \sim x$ .
3. Transitivity: Suppose  $x, y, z \in X$ ,  $x \sim y$  and  $y \sim z$ . Then for  $g_1, g_2 \in G$ ,  $y = g_1x$  and  $z = g_2y$ . Therefore  $z = g_2g_1x$ , and because  $g_2g_1 \in G$ ,  $x \sim z$ .

□

**Definition 6.3** (Orbit). Let  $X$  be a  $G$ -set. For  $x \in X$ , the equivalence class  $[x]$  is called the orbit of  $x$ .

*Remark.* Let  $X$  be a  $G$ -set. Then for each  $x \in X$ ,

$$[x] = G \cdot x := \{g \cdot x \mid g \in G\}.$$

## 7 Finitely generated abelian groups

**Theorem 7.1.** The group  $Z_m \times Z_n \cong Z_{mn}$  iff  $\gcd(m, n) = 1$ .

## 8 Quotient group computations and simple groups

**Definition 8.1.** pass

## 9 Rings and fields

**Definition 9.1** (Ring). A ring  $(R, +, \cdot)$  is a set  $R$  together with the two operations  $+$  and  $\cdot$  such that the following axioms are satisfied:

1.  $(R, +)$  is an abelian group.
2.  $\cdot$  is closed and associative.
3.  $\forall a, b, c \in R$ , the left distributive law  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  and the right distributive law  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$  hold.

**Definition 9.2** (Direct product). Let  $R_1, \dots, R_n$  be rings. The direct product  $R_1 \times \dots \times R_n$  of rings  $R_i$  is a ring under addition and multiplication by components.

**Theorem 9.1.** If  $R$  is a ring, then for any  $a, b \in R$  we have

1.  $0a = a0 = 0$ .
2.  $a(-b) = -(ab) = (-a)b$ .
3.  $(-a)(-b) = ab$

*Proof:* We shall prove these in order.

1. Wlog, because  $a(0 + b) = a0 + ab = ab$  then  $a0 = 0 = 0a$ .
2. Because  $a(b - b) = ab + a(-b) = 0$ , we have  $a(-b) = -ab$ . Similarly,  $(a - a)b = ab + (-a)b = 0$  so  $(-a)b = -ab$ .
3. Because  $-a(b - b) = (-a)b + (-a)(-b) = 0$  we have  $(-a)(-b) = -((-a)b) = ab$ .

□

**Definition 9.3** (Ring homomorphism). For rings  $R$  and  $R'$ , a map  $\phi : R \rightarrow R'$  is a ring homomorphism if the following two conditions are satisfied for all  $a, b \in R$ :

1.  $\phi(a + b) = \phi(a) + \phi(b)$ .
2.  $\phi(ab) = \phi(a)\phi(b)$ .

**Definition 9.4** (Ring isomorphism). A ring isomorphism  $\phi : R \rightarrow R'$  is a ring homomorphism that is bijective. The rings  $R$  and  $R'$  are the isomorphic.

**Definition 9.5** (Commutative ring). A ring in which multiplication is commutative is a commutative ring.

**Definition 9.6** (Unity). An element  $1$  is called the multiplicative identity or unity if  $1a = a = a1$  for all  $a \in R$ .

**Lemma 9.1.** If a ring  $R$  has a unity, then it is unique.

*Proof:* Suppose  $1, 1'$  are both unities of ring  $R$ . Then  $1 \cdot 1' = 1' = 1' \cdot 1 = 1$ . □

*Remark.* Let  $R$  be a ring with unity  $1$ . Then  $1 = 0$  iff  $R$  is a zero ring. This follows from the fact that if  $1 + 1 = 0 + 0 = 0$  then  $R = \{0\}$ .  $\{0\}$  is obviously closed under multiplication.

**Definition 9.7** (Unit). Let  $R$  be a ring with unity  $1 \neq 0$ . An element  $u \in R$  is a unit of  $R$  if there exists  $v \in R$  such that  $vu = 1 = uv$ , where we call  $v$  the multiplicative inverse of  $u$ , denoted by  $u^{-1}$ . Let  $R^\times$  be the set of units in  $R$ , i.e.

$$R^\times := \{u \in R \mid u \text{ is a unit}\}.$$

In other words,  $R^\times$  is the set of elements in  $R$  that have a multiplicative inverse.

*Remark.* Let  $R$  be a ring with unity  $1 \neq 0$ , then  $0 \notin R^\times$ .

*Proof:* By theorem 9.1, for any  $a \in R$ ,  $a0 = 0a = 0$ . □



**Lemma 9.2.** Let  $R$  be a ring with unity  $1 \neq 0$ . If  $u \in R^\times$ , then its multiplicative inverse is unique.

*Proof:* Let  $u \in R$  and  $a, b \in R$  be multiplicative inverses of  $u$ . Then

$$a = a(ub) = (au)b = b.$$

□

**Definition 9.8** (Division ring). A ring with unity  $1 \neq 0$  is called a division ring if  $R^\times = R \setminus \{0\}$ . A noncommutative division ring is called a skew field. A commutative division ring is called a field.

**Definition 9.9** (Subring). A subring of a ring is a subset of the ring that is a ring under induced operations from the whole ring.

## 10 Integral domains

*Remark.* Let  $R$  be a ring in this section.

**Definition 10.1** (0-divisor). An element  $a \in R \setminus \{0\}$  is called a 0-divisor if  $ab = 0$  or  $ba = 0$  for some  $b \in R \setminus \{0\}$ . Let  $ZD(R)$  be the set of 0-divisors of  $R$ . An element  $a \in R \setminus \{0\}$  is called a non-0-divisor if it is not a 0-divisor. Let  $NZD(R)$  be the set of non-0-divisors of  $R$ .

*Remark.*  $a \in NZD(R)$  iff  $ab = ba = 0 \Rightarrow b = 0$ .

*Remark.* The zero ring has no 0-divisors.

**Lemma 10.1.**  $ZD(R) = \emptyset$  for any division ring  $R$ .

*Proof:* Let  $a \in R$  with  $a \neq 0$  and  $b \in ZD(R)$  with  $b^{-1}$  the multiplicative inverse of  $b$ . Then

$$abb^{-1} = 0b^{-1} = 0 = a1 = a.$$

It follows  $a$  is not a unit of  $R$ , a contradiction. □

**Definition 10.2** (Cancellation laws). The cancellation laws hold in  $R$  if  $ab = ac$  with  $a \neq 0$  implies  $b = c$ , and  $ba = ca$  with  $a \neq 0$  implies  $b = c$ .

**Theorem 10.1.** The cancellation laws hold in a ring  $R$  iff  $ZD(R) = \emptyset$ .

*Proof:* To prove the left implication, suppose  $ab = ac$  with  $b \neq c$  and  $a \neq 0$ . Then  $b = (c + g)$  for some  $g \in R$  with  $g \neq 0$ . It follows that  $ac + ag = ac$  and thus  $ag = 0$ , so  $a$  is a zero divisor. To prove the right implication, suppose  $ZD(R) \neq \emptyset$ . Suppose  $a, c \in R$  and  $g \in ZD(R)$  with  $ag = 0$ . Then  $ac + ag = ac$  and  $a(c + g) = ac$ . But  $c + g \neq c$ , so cancellation laws do not hold. □

**Definition 10.3** (Integral domain). An integral domain  $D$  is a commutative ring with unity  $1 \neq 0$  and  $ZD(R) = \emptyset$ .

*Remark.* Every field is an integral domain.

**Theorem 10.2.** Every finite integral domain is a field.

*Proof:* Cancellation laws imply the function  $\delta_a$  with  $a \in R$  and  $a \neq 0$  defined by

$$\begin{aligned} \delta_a : R &\rightarrow R \\ x &\rightarrow ax \end{aligned}$$

is onto. Because  $|R| < \infty$ ,  $\delta_a$  is surjective. Thus for every element of  $a \neq 0$ , there exists an element  $b \in R$  such that  $ab = ba = 1$ . □

**Theorem 10.3.** Let  $R$  be a ring and  $R^\times$  the set of units in  $R$ . Then  $(R^\times, \cdot)$  is a group.

*Proof:* Every element clearly has an inverse, and 1 is an identity element. Because  $R$  is a ring we know that  $\cdot$  is associative. □

**Definition 10.4.** For  $n \in \mathbb{Z}^+$ , define

$$G_n := Z_n^\times = \{a \in Z_n \mid \gcd(a, n) = 1\}.$$

**Definition 10.5** (Euler phi-function). The Euler phi-function  $\phi : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  is defined

$$\phi(n) = |\{a \in \{1, \dots, n\} \mid \gcd(a, n) = 1\}|.$$

**Lemma 10.2.** For  $n \in \mathbb{Z}^+$ ,

$$\phi(n) = |Z_n^\times|.$$

**Lemma 10.3.** If  $a \in Z_n^+$ , then  $a^{|Z_n^+|} = 1$ .

*Proof:*

□

**Theorem 10.4** (Euler's Theorem). Let  $n \in \mathbb{Z}^+$ . Then  $a^{\phi(n)} \equiv 1 \pmod{n}$  for any  $a \in \mathbb{Z}$  with  $\gcd(a, n) = 1$ .

*Proof:* Let  $a, n \in \mathbb{Z}^+$ , with  $\gcd(a, n) = 1$ . If  $n = 1$ , clearly  $a^{\phi(n)} = a^1 = a$ , and  $a \equiv a \pmod{n}$ . If  $n > 1$ , because  $n$  and  $a$  are relatively prime we know that for  $q, r \in \mathbb{N}$  with  $0 < r < n$  that  $a = qn + r$ , and that  $\gcd(r, n) = 1$ . Therefore  $r \in Z_n^\times$ , and by Lagrange's theorem  $r^{\phi(n)} = r^{|Z_n^\times|} = r^{|r| \cdot |Z_n^\times| / \langle r \rangle} \equiv 1 \pmod{n}$ . Therefore  $a^{\phi(n)} \equiv 1 \pmod{n}$ . □

**Theorem 10.5** (Fermat's little theorem). Let  $a \in \mathbb{Z}$  and  $p$  be a prime. If  $p$  does not divide  $a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

**Definition 10.6** (Mersenne primes). Primes of the form  $2^p - 1$  where  $p$  is prime are known as Mersenne primes.

**Theorem 10.6.** Let  $n \in \mathbb{Z}^+$ . Let  $a, b \in Z_n$ . The equation  $ax = b$  has a unique solution in  $Z_n$  iff  $\gcd(a, n) = 1$ .

## 11 The quotient field of an integral domain

*Remark.* In this section, let  $D$  be an integral domain and

$$S := \{(a, b) \mid a, b \in D \text{ and } b \neq 0\} = D \times (D \setminus \{0\}) = D \times NZD().$$

**Definition 11.1.** Define a relation  $\sim$  on  $S$  as follows: for  $(a, b), (c, d) \in S$  we say  $(a, b) \sim (c, d)$  if  $ad = bc$ .

*Remark.*  $\sim$  is an equivalence relation.

**Definition 11.2.** In this section, let  $F$  be the set of equivalence classes with respect to  $\sim$ ,

$$F := S / \sim = \{[(a, b)] \mid (a, b) \in S\}.$$

**Definition 11.3.** For  $[(a, b)], [(c, d)] \in F$ , the equations

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

and

$$[(a, b)][(c, d)] = [(ac, bd)]$$

Give well-defined operations of addition and multiplication on  $F$ .

**Theorem 11.1.**  $(F, +, \cdot)$  is a field.

**Lemma 11.1.** We have an injective ring homomorphism

$$i : D \rightarrow Fa \rightarrow [(a, 1)].$$

Thus,  $D$  can be regarded as a subring of  $F$ .

**Theorem 11.2.** Any integral domain  $D$  can be embedded in a field  $F$  such that every element of  $F$  can be expressed as a quotient of two elements of  $D$ . Such a field  $F$  is a quotient field of  $D$ , and denoted by  $Q(D)$ .

## 12 Ideals and quotient rings

**Definition 12.1** (Kernel). Let  $\phi : R \rightarrow R'$  be a ring homomorphism. The subring

$$\text{Ker}(\phi) := \phi^{-1}(0') = \{a \in R \mid \phi(a) = 0'\}$$

is the kernel of  $\phi$ .

**Theorem 12.1.** Let  $\phi : R \rightarrow R'$  be a ring homomorphism with  $\text{Ker}(\phi) := H$ . Let  $a \in R$ . Then

$$\phi^{-1}(\{\phi(a)\}) = a + H = H + a.$$

**Definition 12.2** (Ideal). An additive subgroup  $N$  of a ring  $R$  satisfying the properties  $aN \subseteq N$  and  $Nb \subseteq N$  for all  $a, b \in R$  is called an ideal, denoted by  $N \leq R$ .

*Remark.* If  $R \neq \{0\}$ , then  $aN$  is not a coset, because 0 has no multiplicative inverse.

**Lemma 12.1.** If  $R$  is a ring and  $N \leq R$ , then  $N$  is a subring of  $R$ .

**Theorem 12.2.** Let  $H$  be a subring of  $R$ . Multiplication of additive cosets of  $H$  is well-defined by the equation

$$(r + H)(s + H) = rs + H$$

iff  $H \leq R$ .

*Proof:* To prove the right implication, suppose that  $H \leq R$ . Then for  $h_1, h_2 \in H$ ,  $(r + H)(s + H) = (r + h_1 + H)(s + h_2 + H) = (r + h_1)(s + h_2) + H$ . Because  $H \leq R$ , we know that  $rh_2 + sh_1 + h_1h_2 \in H$ , therefore  $rs + rh_2 + sh_1 + h_2h_1 + H = rs + H$ . To prove the left implication, suppose this operation is well-defined. The left implication will be proven later by me :)  $\square$

**Corollary 12.1.** Let  $N$  be an ideal of a ring  $R$ . Then  $R/N, +, \cdot$  forms a ring. This is called the factor ring (or quotient ring) of  $R$  and  $N$ . This follows from the fact  $H \leq R$ , thus  $H/R$  is an abelian group, and that  $H/R$  is well-defined under the operation given above.

**Theorem 12.3.** Let  $\phi : R \rightarrow R'$  be a ring homomorphism. If  $H \subseteq R$  is a subring, then as subrings  $\phi(H) \subseteq \phi(R) \subseteq R'$ . Also, if  $H' \subseteq R'$  is a subring, then  $\phi^{-1}(H') \subseteq R$  is a subring.

**Theorem 12.4.** Let  $\phi : R \rightarrow R'$  be a ring homomorphism. If  $I \leq R$ , then  $\phi(I) \leq \phi(R)$ . Also, if  $I' \leq R'$ , then  $\phi^{-1}(I') \leq R$ .

**Theorem 12.5** (1st ring isomorphism theorem). Let  $\phi : R \rightarrow R'$  be a ring homomorphism with  $\text{Ker}(\phi) =: N$ . Then  $N \leq R$  and there is a ring isomorphism

$$\begin{aligned} \mu : R/N &\rightarrow \phi(R) \\ a + N &\rightarrow \phi(a). \end{aligned}$$

**Theorem 12.6** (4th ring isomorphism theorem). Let  $R$  be a ring,  $I \leq R$ , and  $\pi : R \rightarrow R/I$  the natural projection. Then there is a bijection:

$$\{S \mid S \subseteq R/I \text{ is a subring}\} \leftrightarrow \{J \mid I \subseteq J \subseteq R \text{ are subrings}\}.$$

*Proof:*

$\square$

**Definition 12.3** (Proper ideal). A proper ideal is any ideal that is a strict subset of the ring.

**Definition 12.4** (Maximal ideal). Let  $R$  be a ring. A proper ideal  $m \leq R$  if for all  $J \leq R$  we have

$$m \subseteq J \Rightarrow J = m \vee J = R.$$

**Theorem 12.7.** Let  $R$  be a commutative ring with unity  $1 \neq 0$ . Then  $m \leq R$  is a maximal ideal iff  $R/m$  is a field.

**Definition 12.5.** Let  $R$  be a commutative ring. We say that a proper ideal  $p \leq R$  is a prime ideal if  $ab \in p$  for  $a, b \in R$  then  $a \in p$  or  $b \in p$ , i.e.  $ab \in R \setminus p$  for any  $a, b \in R \setminus p$ .

**Definition 12.6.** Let  $R$  be an integral domain.

1. An element  $r \in R \setminus \{R^\times \cup \{0\}\}$  is irreducible in  $R$  if  $r = ab$  with  $a, b \in R$  implies  $a \in R^\times$  or  $b \in R^\times$ . Otherwise,  $r$  is said to be reducible.
2. An element  $p \in R \setminus \{R^\times \cup \{0\}\}$  is prime in  $R$  if  $pR \leq R$  is a prime ideal.

*Remark.* In an integer domain  $R$ , a prime,  $p \in R$  is always irreducible.

**Lemma 12.2.** Let  $R$  be a commutative ring with unity  $1 \neq 0$ . Then  $p \leq R$  is a prime ideal iff  $R/p$  is an integral domain.

**Definition 12.7.** An integral domain  $R$  is a PID if every ideal  $I$  of  $R$  can be written in the form  $xR$  for some  $x \in R$ .

*Remark.*  $\mathbb{Z}$  is a PID.

**Definition 12.8.** Let  $R$  be a ring and  $I, J \leq R$ .

1. The sum  $I + J$  of  $I$  and  $J$  is defined by

$$I + J = \{a + b \mid a \in I \text{ and } b \in J\}.$$

2. The product  $IJ$  of  $I$  and  $J$  is defined by

$$IJ = \left\{ \sum_i^{\text{finite}} a_i b_i \mid a_i \in I \text{ and } b_i \in J \right\}.$$

*Remark.*  $I + J, IJ \leq R$ .

**Theorem 12.8.**  $\mathbb{R}[x]$  is a PID.

**Lemma 12.3.** Let  $R$  be a PID.  $p \leq R$  is a prime ideal iff it is a maximal ideal.

**Lemma 12.4.** In a PID  $R$ ,  $p \in R \setminus \{R^\times \cup \{0\}\}$  is prime iff it is irreducible.