Abstract Algebra

Mark Sullivan

March 8, 2019

Contents

1 Properties of $\mathbb{Z}$

1.1 Dictionary of terms and notations

Definition 1.1 *Let $a, b \in \mathbb{Z}$ such that $a \neq 0$. We say that <u>a divides b</u>, that <u>a is a factor of b</u>, that <u>a is a divisor of b</u>, or that <u>b is a multiple of a</u> provided that $\exists\, q \in \mathbb{Z}$ such that $b = qa$.*

Notation We denote the statement "a divides b" by "$a|b$."

Definition 1.2 *Let $p \in \mathbb{Z}^+$. We say that the number p is a <u>prime number</u> provided that $\forall\, n \in \mathbb{Z}^+$, if $n|p$, then $n = 1$ or $n = p$.*

Definition 1.3 *Let $a, b \in \mathbb{Z} \setminus \{0\}$. The <u>greatest common divisor of a and b</u> is the greatest element of the set $\left\{ d \in \mathbb{Z} \middle| d|a \text{ and } d|b \right\}$.*

Notation Given $a, b \in \mathbb{Z} \setminus \{0\}$, we denote the greatest common divisor of a and b by "$\gcd(a, b)$."

Definition 1.4 *Let $a, b \in \mathbb{Z} \setminus \{0\}$. We say that <u>$a$ and b are relatively prime</u> provided that $\gcd(a, b) = 1$.*

Definition 1.5 *Let $a, b \in \mathbb{Z} \setminus \{0\}$. The <u>least common multiple of a and b</u> is the least element of the set $\left\{ m \in \mathbb{Z} \middle| a|m \text{ and } b|m \right\}$.*

Definition 1.6 *Let $n \in \mathbb{Z}^+$. Given $a, b \in \mathbb{Z}$, we say that <u>a is congruent to b modulo n</u> provided that $n|a - b$.*

Notation Given $a, b, n \in \mathbb{Z}$ such that $n > 0$, we denote the statement "a is congruent to b modulo n" by "$a \equiv b \pmod{n}$."

1.1.1 Important theorems

The following is known as the well-ordering principle.

Theorem 1.7 *Given* $S \subseteq \mathbb{Z}^+$*, if* $S \neq \varnothing$*, then* $\exists\, t \in S$ *such that* $\forall\, x \in S$*,* $t \leq x$*.*

The following is known as the division algorithm.

Theorem 1.8 *Let* $a, b \in \mathbb{Z}$ *such that* $b > 0$*. There exist unique* $q, r \in \mathbb{Z}$ *such that* $a = bq + r$ *and* $0 \leq r \leq b$*.*

The following is known as Bézout's lemma or Bézout's identity.

Theorem 1.9 *Given* $a, b \in \mathbb{Z} \setminus \{0\}$*,* $\exists\, s, t \in \mathbb{Z}$ *such that* $as + bt = \gcd(a, b)$*.*

The following is known as Euclid's lemma.

Theorem 1.10 *Let* $a, b, p \in \mathbb{Z}$*. If* p *is a prime number and* $p|ab$*, then* $p|a$ *or* $p|b$*.*

The following is known as the fundamental theorem of arithmetic.

Theorem 1.11 *Let* $n \in \mathbb{Z}$ *such that* $n > 1$*. The following statements are true.*
(i) There exist prime numbers $p_1, p_2, ..., p_r \in \mathbb{Z}^+$ *such that* $n = p_1 p_2 ... p_r$*.*
(ii) If $q_1, q_2, ..., q_s \in \mathbb{Z}^+$ *are prime numbers such that* $n = q_1 q_2 ... q_s$*, then for each* $j \in \{1, 2, ..., s\}$*,* $\exists\, i \in \{1, 2, ..., r\}$ *such that* $q_j = p_i$*.*

The following is known as the principle of mathematical induction.

Theorem 1.12 *Let* $S \subseteq \mathbb{Z}^+$ *such that* $S \neq \varnothing$*. If* $1 \in S$ *and* $\forall\, n \in S$*,* $n + 1 \in S$*, then* $S = \mathbb{Z}^+$*.*

2 Group theory

2.1 Dictionary of terms and notations

Definition 2.1 *Let S be a set. A binary operation on S is a function $* : S \times S \to S$.*

Notation Given a binary operation $*$ on a set S and $x, y \in S$, we will often denote $*(x, y)$ as "$x * y$" or simply "xy."

Definition 2.2 *Let S be a set, and let $*$ be a binary operation on S. We say that $*$ is an associative binary operation provided that $\forall\, x, y, z \in S$,*

$$x * (y * z) = (x * y) * z. \tag{1}$$

Definition 2.3 *Let G be a nonempty set, and let $*$ be a binary operation on G. We say that $(G, *)$ is a group provided that the following statements are true.*
(i) $*$ is associative.
(ii) $\exists\, e \in G$ such that $\forall\, a \in G$, $a * e = e * a = a$.
(iii) $\forall\, a \in G$, $\exists\, b \in G$ such that $a * b = b * a = e$.

Notation We will often write the statement "$(G, *)$ is a group" as "G is a group under $*$," or simply "G is a group."

Definition 2.4 *Let G be a group. An identity element of G is an element $e \in G$ such that $\forall\, a \in G$, $a * e = e * a = a$.*

Definition 2.5 *Let G be a group, and let $e \in G$ be the identity element of G. Given $a \in G$, an inverse element of a in G is an element $b \in G$ such that $a * b = b * a = e$.*

Notation Given a group G and $a \in G$, will often denote the inverse element of a by "a^{-1}."

Definition 2.6 *Let G be a group. We say that G is a trivial group provided that $|G| = 1$.*

Definition 2.7 *Let $n \in \mathbb{Z}^+$. The dihedral group of order $2n$ is the group of isometries of a regular polygon with n sides.*

Notation We denote the dihedral group of order $2n$ by "D_n."

Definition 2.8 *Let $n \in \mathbb{Z}^+$. Define an equivalence relation $\equiv$ on $\mathbb{Z}$ such that $\forall\ a, b \in \mathbb{Z}$, $a \equiv b$ if and only if $a \equiv b \pmod{n}$. The group of integers modulo n is the quotient set ${}^{\mathbb{Z}}/_{\equiv}$ under the binary operation defined via the relationship $[a] + [b] = [a + b]$.*

Notation Given $n \in \mathbb{Z}^+$, we denote the group of integers modulo n by "${}^{\mathbb{Z}}/_{n}$," "${}^{\mathbb{Z}}/_{n\mathbb{Z}}$," or "$\mathbb{Z}_n$."

Definition 2.9 *Let $n \in \mathbb{Z}^+$. The group of units modulo n is the set*

$$U(n) = \left\{ [a] \in {}^{\mathbb{Z}}/_{n} \middle| \gcd(a, n) = 1 \right\} \tag{2}$$

under the binary operation defined via the relationship $[a] \cdot [b] = [ab]$.

Definition 2.10 *Let Ω be a set. A permutation of Ω is a bijection $\sigma : \Omega \to \Omega$.*

Definition 2.11 *Let Ω be a nonempty set. The symmetric group based on Ω is the group $(S_\Omega, \circ)$, where*

$$S_\Omega = \left\{ \sigma : \Omega \to \Omega \middle| \sigma \textit{ is a bijection} \right\}. \tag{3}$$

Notation Given $\sigma \in S_\Omega$, we define $\sigma^1 = \sigma$ and for each $n \in \mathbb{Z}^+$, $\sigma^{n+1} = \sigma \circ \sigma^n$.

Definition 2.12 *Let $n \in \mathbb{Z}^+$. The symmetric group of degree n is the symmetric group S_X, where $X = \{1, 2, ..., n\}$.*

Notation We denote the symmetric group of degree n by "S_n."

Definition 2.13 *Let Ω be a set. A cycle in S_Ω is a permutation $\sigma \in S_\Omega$ such that $\forall\ a, b \in \Omega$, if $\sigma(a) \neq a$ and $\sigma(b) \neq b$, then $\exists\ r \in \mathbb{Z}^+$ such that $\sigma^r(a) = b$.*

Definition 2.14 *Let Ω be a set, and let $\sigma \in S_\Omega$ be a cycle. The length of σ is the cardinality $\left| \left\{ x \in \Omega \middle| \sigma(x) \neq x \right\} \right|$.*

Definition 2.15 *Let Ω be a set. Given a cycle $\sigma \in S_\Omega$ and $k \in \mathbb{Z}^+$, we say that σ is a k-cycle in S_Ω provided that the length of σ is k.*

Notation Given a k-cycle $\sigma \in S_\Omega$ and $a \in \Omega$ such that $\sigma(a) \neq a$, we will often write

$$\sigma = \begin{pmatrix} a & \sigma(a) & \sigma^2(a) & \ldots & \sigma^{k-1}(a) \end{pmatrix}. \tag{4}$$

Definition 2.16 *Let Ω be a set. Given cycles $\sigma, \tau \in S_\Omega$, we say that σ and τ are disjoint cycles provided that $\left\{x \in \Omega \middle| \sigma(x) \neq x\right\} \cap \left\{x \in \Omega \middle| \tau(x) \neq x\right\} = \varnothing$.*

Definition 2.17 *Let Ω be a set. A transposition in S_Ω is a 2-cycle in S_Ω.*

Definition 2.18 *The group of unit quaternions is the group $(Q_8, \cdot)$, where*

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}, \tag{5}$$

and $\cdot$ is defined so that $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, and $ki = j$.

Definition 2.19 *Let $n \in \mathbb{Z}^+$, and let K be a field. The general linear group of degree n over K is the group $\mathrm{GL}_n(K)$ of $n \times n$ invertible matrices with entries in K, under matrix multiplication.*

Definition 2.20 *Let $n \in \mathbb{Z}^+$, and let K be a field. The special linear group of degree n over K is the group $\mathrm{SL}_n(K)$ of $n \times n$ matrices with entries in K and determinant 1, under matrix multiplication.*

Definition 2.21 *Let G be a group. We say that G is a cyclic group provided that $\exists\, a \in G$ such that $\forall\, b \in G$, $b = a^n$ for some $n \in \mathbb{Z}$.*

Definition 2.22 *Let S be a set, and let $*$ be a binary operation on S. We say that $*$ is a commutative binary operation provided that $\forall\, x, y \in S$, $x * y = y * x$.*

Definition 2.23 *Let $(G, *)$ be a group. We say that G is an Abelian group provided that $*$ is a commutative binary operation.*

Definition 2.24 *Let G be a group. The order of G is the cardinality $|G|$.*

Definition 2.25 *Let G be a group, and let $a \in G$. We say that a has finite order in G provided that $\exists\, n \in \mathbb{Z}^+$ such that $a^n = e$, where $e \in G$ is the identity element of G.*

Definition 2.26 *Let G be a group, and let $a \in G$. We say that a has infinite order in G provided that $\forall\, n \in \mathbb{Z}^+$, a^n is not the identity element of G.*

Definition 2.27 *Let G be a group, and let $a \in G$ have finite order in G. Suppose that $e \in G$ is the identity element of G. The order of a is the least element $n \in \mathbb{Z}^+$ such that $a^n = e$.*

Notation Given a group G and $a \in G$, we denote the order of a by "$|a|$."

Definition 2.28 *Let $f : X \to Y$ be a function, and let $S \subseteq X$. The restriction map of f to S is the function $f\big|_S : S \to Y$ via $f\big|_S(x) = f(x)$.*

Definition 2.29 *Let $(G, *)$ be a group. Given a nonempty $H \subseteq G$, we say that H is a subgroup of G [with respect to $*$] provided that H is a group under $*\big|_{H\times H}$.*

Notation We will sometimes denote the statement "H is a subgroup of G" by "$H \le G$."

Definition 2.30 *Let G be a group, and let $a \in G$. The cyclic group generated by a is the group $\langle a\rangle = \left\{a^n \middle| n \in \mathbb{Z}\right\}$.*

Definition 2.31 *Let G be a group. The center of G is the subset*

$$Z(G) = \left\{a \in G \middle| \forall\, x \in G,\ ax = xa\right\}. \tag{6}$$

Definition 2.32 *Let G be a group. Given $a \in G$, the centralizer of a in G is the set*

$$C(a) = \left\{x \in G \middle| ax = xa\right\}. \tag{7}$$

Definition 2.33 *Let G be a group, and let H be a subgroup of G. Given $a \in G$, the left coset of G by H containing a is the set*

$$a * H = \left\{a * h \in G \middle| h \in H\right\}. \tag{8}$$

Definition 2.34 *Let G be a group, and let H be a subgroup of G. Given $a \in G$, the right coset of G by H containing a is the set*

$$H * a = \left\{ h * a \in G \middle| h \in H \right\}. \tag{9}$$

Notation We will often denote a coset $a * N$ by "aN," and $N * a$ by "Na."

Definition 2.35 *Let G be a group. Given a subgroup N of G, we say that N is a normal subgroup of G provided that $\forall\, a \in G$, $aN = Na$.*

Notation We will often denote the statement "N is a normal subgroup of G" as "$N \triangleleft G$."

Definition 2.36 *Let G be a group, and let H be a subgroup of G. The quotient space of G by H is the set*

$$G/H = \left\{ aH \middle| a \in G \right\}. \tag{10}$$

Definition 2.37 *Let G be a group, and let H be a subgroup of G. The coset multiplication in G/H is the binary operation $*$ on G/H defined via $aH * bH = abH$.*

Definition 2.38 *Let G be a group, and let $N \triangleleft G$. The quotient group of G by N is the group G/N under coset multiplication.*

Definition 2.39 *Let G_1 and G_2 be groups, and let $\varphi : G_1 \to G_2$ be a function. We say that φ is a [group] homomorphism provided that $\forall\, a, b \in G_1$,*

$$\varphi(ab) = \varphi(a)\,\varphi(b). \tag{11}$$

Definition 2.40 *Let $\varphi : G_1 \to G_2$ be a homomorphism. Suppose that $e_2 \in G_2$ is the identity element of G_2. The kernel of φ is the set*

$$\ker \varphi = \left\{ a \in G_1 \middle| \varphi(a) = e_2 \right\} \tag{12}$$

Definition 2.41 *Let $\varphi : G_1 \to G_2$ be a homomorphism. The image or range of φ is the set*

$$\operatorname{Im} \varphi = \left\{ \varphi(a) \in G_2 \middle| a \in G_1 \right\}. \tag{13}$$

Definition 2.42 *Let $\varphi : G_1 \to G_2$ be a homomorphism. We say that φ is a monomorphism provided that φ is injective.*

Definition 2.43 *Let $\varphi : G_1 \to G_2$ be a homomorphism. We say that φ is an epimorphism provided that φ is surjective.*

Definition 2.44 *Let $\varphi : G_1 \to G_2$ be a group homomorphism. We say that φ is a group isomorphism provided that there exists a group homomorphism $\psi : G_2 \to G_1$ such that $\psi \circ \varphi = \mathrm{id}_{G_1}$ and $\varphi \circ \psi = \mathrm{id}_{G_2}$.*

Definition 2.45 *Let $\varphi : G_1 \to G_2$ be a group homomorphism. We say that G_1 and G_2 are isomorphic [as groups] provided that there exists a group isomorphism $\varphi : G_1 \to G_2$.*

Notation We may denote the statement "G_1 and G_2 are isomorphic groups" by "$G_1 \simeq G_2$."

2.2 Examples

Example 2.46 *The following are examples of groups.*

(i) $\mathbb{Z}$ *under addition.*

(ii) $\mathbb{Q}$ *under addition.*

(iii) $\mathbb{R}$ *under addition.*

(iv) $\mathbb{C}$ *under addition.*

(v) $\mathbb{Q} \setminus \{0\}$ *under multiplication.*

(vi) $\mathbb{R} \setminus \{0\}$ *under multiplication.*

(vii) $\mathbb{C} \setminus \{0\}$ *under multiplication.*

(viii) $\{0\}$ *under addition (or multiplication). This is a trivial group.*

(ix) Given $n \in \mathbb{Z}^+$ *and* $a \in \mathbb{C}$ *such that* $a^n = 1$*, the set*

$$G = \left\{1, a, a^2, a^3, ..., a^{n-1}\right\} \tag{14}$$

is a group under multiplication. This is a cyclic group.

(x) Any vector space is a group.

(xi) All of the groups above are abelian groups. Given $n \in \mathbb{Z}^+$*, the symmetric group* S_n *is a non-abelian group. The dihedral group* D_{2n}*, the group of unit quaternions* Q_8*, the general linear group* $\mathrm{GL}_n(\mathbb{C})$*, and the special linear group* $\mathrm{SL}_n(\mathbb{C})$ *are also non-abelian groups.*

Example 2.47 *The following are examples of subgroups.*

(i) $\mathbb{Z}$ *is a subgroup of* $\mathbb{Q}$*.*

(ii) $\mathbb{Q}$ *is a subgroup of* $\mathbb{R}$*.*

(iii) $\mathbb{R}$ *is a subgroup of* $\mathbb{C}$*.*

(iv) $\mathrm{SL}_n(K)$ *is a subgroup of* $\mathrm{GL}_n(K)$*.*

(v) Every group contains a trivial subgroup.

(vi) Every group is a subgroup of itself.

2.3 Propositions

Proposition 2.48 *Let G be a group. Given $e_1, e_2 \in G$, if e_1 and e_2 are both identity elements of G, then $e_1 = e_2$.*

Proof Since e_2 is an identity element of G, we can say that $e_1e_2 = e_1$. At the same time, since e_1 is an identity element of G, we have that $e_1e_2 = e_2$. Thus, $e_1 = e_1e_2 = e_2$. $\square$

Proposition 2.49 *Let G be a group, and let $e \in G$ be the identity element of G. If $\forall\, a, b \in G$, $ab = e$, then $G = \{e\}$.*

Proof Let $a \in G$. We know that $ae = a$, and by assumption, $ae = e$. Thus, $a = ae = e$. $\square$

Proposition 2.50 *Let G be a group. Given $a, b, c \in G$, if $ac = bc$, then $a = b$. Similarly, if $ca = cb$, then $a = b$.*

Proof Suppose that $ac = bc$. Since G is a group, $\exists\, c^{-1} \in G$ such that $cc^{-1} = e$, where $e \in G$ is the identity element of G. Thus,

$$a = ae = acc^{-1} = bcc^{-1} = be = b. \tag{15}$$

The proof for $ca = cb$ is similar. $\square$

Proposition 2.51 *Let G be a group. Given $a, b \in G$, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.*

Proof ($\Rightarrow$) Assume that $(ab)^2 = a^2b^2$. This means that $abab = aabb$. Since G is a group, $\exists\, b^{-1} \in G$ such that $bb^{-1} = e$, where $e \in G$ is the identity element of G. At the same time, $\exists\, a^{-1} \in G$ such that $a^{-1}a = e$. Therefore,

$$ba = ebae = a^{-1}ababb^{-1} = a^{-1}aabbb^{-1} = eabe = ab. \tag{16}$$

($\Leftarrow$) Assume that $ab = ba$. In that case, $aab = aba$, and so $aabb = abab$, hence $a^2b^2 = (ab)^2$. $\square$

Proposition 2.52 *Let G be a group, and let $e \in G$ be the identity element of G. Given $a, b, c \in G$, if $ab = ba = e$ and $ac = ca = e$, then $b = c$.*

Proof Suppose that $ab = ba = e$ and $ac = ca = e$. This means that $ab = ac$. By Proposition 2.50, we deduce that $b = c$. $\square$

Proposition 2.53 *Let G be a group. Given $a \in G$, $(a^{-1})^{-1} = a$.*

Proof Define $b = a^{-1}$. We know that $ab = e$. Therefore,

$$a = ae = abb^{-1} = eb^{-1} = b^{-1} = \left(a^{-1}\right)^{-1}. \tag{17}$$

$\square$

Proposition 2.54 *Let G be a group, and let $e \in G$ be the identity element of G. Given $a \in G$, if $a^{-1} = e$, then $a = e$.*

Proof Suppose that $a^{-1} = e$. This implies that

$$e = aa^{-1} = ae = a. \tag{18}$$

$\square$

Proposition 2.55 *Let G be a group. Given $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof We notice that

$$(ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a^{-1} = aea^{-1} = aa^{-1} = e, \tag{19}$$

and

$$\left(b^{-1}a^{-1}\right)(ab) = b^{-1}\left(a^{-1}a\right)b = b^{-1}eb = b^{-1}b = e. \tag{20}$$

Thus, $b^{-1}a^{-1}$ is the inverse element of ab. $\square$

Proposition 2.56 *Let G be a group. Given $a_1, a_2, ..., a_n \in G$,*

$$(a_1a_2...a_n)^{-1} = {a_n}^{-1}...{a_2}^{-1}{a_1}^{-1}. \tag{21}$$

Proof We proceed by mathematical induction on n. First, $(a_1)^{-1} = {a_1}^{-1}$, trivially. This establishes a basis for induction. Assume, as the induction hypothesis, that for some $k \in \mathbb{Z}^+$, $(a_1a_2...a_k)^{-1} = {a_k}^{-1}...{a_2}^{-1}{a_1}^{-1}$. Proposition 2.55 indicates that

$$(a_1a_2...a_ka_{k+1})^{-1} = ((a_1a_2...a_k)\,a_{k+1})^{-1} = {a_{k+1}}^{-1}(a_1a_2...a_k)^{-1}. \tag{22}$$

Therefore,

$$(a_1a_2...a_ka_{k+1})^{-1} = {a_{k+1}}^{-1}\left({a_k}^{-1}...{a_2}^{-1}{a_1}^{-1}\right) = {a_{k+1}}^{-1}{a_k}^{-1}...{a_2}^{-1}{a_1}^{-1}. \tag{23}$$

This completes the induction. $\square$

Proposition 2.57 *Let G be a group. Given a nonempty $H \subseteq G$, H is a subgroup of G if and only if $\forall\ a, b \in H$, $ab^{-1} \in H$.*

Proof Let $(G, *)$ be a group, and let $H \subseteq G$ be nonempty.

($\Rightarrow$) Assume that H is a subgroup of G. Let $a, b \in H$. In that case, $b^{-1} \in H$, since H is a group. Therefore, $a * b^{-1} \in H$.

($\Leftarrow$) Assume that $\forall\ a, b \in H$, $a * b^{-1} \in H$. We will show that H is a subgroup of G. First, we know that $*\big|_{H\times H}$ is associative, since $*$ is associative. As $H \neq \varnothing$, we know that $\exists\ a \in H$. By assumption, $e = a * a^{-1} \in H$, where $e \in G$ is the identity element of G. Now, $\forall\ b \in G$, $b * e = e * b = b$, so in particular, $\forall\ b \in H$, $b * e = e * b = b$. This shows that H contains an identity element. Given $a \in H$, we know that $a^{-1} = e * a^{-1} \in H$ by assumption. This shows that for each element of H, an inverse element exists in H.

We claim that $*\big|_{H\times H}$ is a binary operation on H (or in other words, that H is closed under $*$). Given $a, b \in H$, we know that $b^{-1} \in H$. Therefore, by assumption, $a * \left(b^{-1}\right)^{-1} \in H$. By Proposition 2.53, this implies that $a * b \in H$.

As H satisfies the conditions of a group, we deduce that H is a subgroup of G. □

Proposition 2.58 *Let G be a group, and let $a \in G$. Given a subgroup H of G, if $a \in H$, then $\langle a\rangle \subseteq H$.*

Proof Let H be a subgroup of G. Let $a \in H$. We claim that $\forall\, n \in \mathbb{Z}^+$, $a^n \in H$. We proceed by mathematical induction on n. First, we note that $a^1 = a \in H$. This establishes a basis for induction. Assume, as the induction hypothesis, that $a^k \in H$ for some $k \in \mathbb{Z}^+$. Now $a^{k+1} = a^k a \in H$, since H is a group. This completes the induction.

We know that $e \in H$, since H is a subgroup of G. Thus, $a^0 \in H$. Further, for each $n \in \mathbb{Z}^+$, $a^{-n} \in H$, since $a^{-n} = (a^n)^{-1}$, and H is a group. Therefore, $\langle a\rangle = \left\{a^n \middle| n \in \mathbb{Z}\right\} \subseteq H$. □

Proposition 2.59 *Let G be a group, and let $a \in G$. Suppose that $e \in G$ is the identity element of G. Given $n \in \mathbb{Z}$, $a^n = e$ if and only if $|a|$ divides n.*

Proof Let $a \in G$, and let $n \in \mathbb{Z}$. Define $k = |a|$.

($\Rightarrow$) Assume that $a^n = e$. We know from Theorem 1.8 that $\exists\, q, r \in \mathbb{Z}$ such that $n = kq + r$ and $0 \leq r < k$. Therefore,

$$e = a^n = a^{kq+r} = a^{kq}a^r = \left(a^k\right)^q a^r = e^q a^r = a^r. \tag{24}$$

Since $r < k$, and k is the least element of $\mathbb{Z}^+$ such that $a^k = e$, we must have that $r \notin \mathbb{Z}^+$; $r = 0$. Thus, $n = kq$, and so $k|n$.

($\Leftarrow$) Assume that $k|n$. In that case, $\exists\, q \in \mathbb{Z}$ such that $n = kq$. Thus,

$$a^n = a^{kq} = \left(a^k\right)^q = e^q = e. \tag{25}$$

$\square$

Proposition 2.60 *Let G be a group. Given $a \in G$, $\left|a^{-1}\right| = |a|$.*

Proof Let $a \in G$, and define $|a| = k$ for some $k \in \mathbb{Z}^+$. Define $l = \left|a^{-1}\right|$. Assume, with the expectation of a contradiction, that $l \neq k$. We notice that

$$e = e^k = \left(aa^{-1}\right)^k = a^k\left(a^{-1}\right)^k = e\left(a^{-1}\right)^k = \left(a^{-1}\right)^k, \tag{26}$$

where $e \in G$ is the identity element of G. This shows that $l \leq k$, so $l < k$. Now, we notice that $a^l \neq e$, so

$$e = e^l = \left(a^{-1}a\right)^l = \left(a^{-1}\right)^l a^l = ea^l = a^l \neq e. \tag{27}$$

This contradiction leads us to conclude that our assumption that $l \neq k$ is false; $l = k$. $\square$

Proposition 2.61 *Let G be a group, and let $a \in G$. If a has finite order in G, then $|a| = \left|\langle a \rangle\right|$. If a has infinite order in G, then $\langle a \rangle$ is an infinite set.*

Proof Let $a \in G$, and suppose that a has finite order in G. Define $k = |a|$. Let $S = \left\{a, a^2, ..., a^k\right\}$.

We claim that $S = \langle a \rangle$. First, it is clear that $S \subseteq \langle a \rangle$, by definition. Now, suppose that $x \in \langle a \rangle$. In that case, $x = a^n$ for some $n \in \mathbb{Z}$. We note that $n \equiv m \pmod{k}$ for some $m \in \{1, 2, ..., k\}$, since congruence modulo k is an equivalence relation. In that case, $k|n - m$. We deduce that $a^{n-m} = e$, by Proposition 2.59. Ergo, $x = a^n = a^m \in S$.

Since $\langle a \rangle = S$, and $|S| = k$, $\left|\langle a \rangle\right| = k = |a|$. $\square$

Proposition 2.62 *Let G be a group, and let $a \in G$. Suppose that $|a| = k$ for some $k \in \mathbb{Z}^+$. Given $l \in \mathbb{Z}^+$, $\left\langle a^l \right\rangle = \left\langle a^{\gcd(k,l)} \right\rangle$.*

Proof Define $d = \gcd(k, l)$, and let $l = qd$ for some $q \in \mathbb{Z}$.

($\subseteq$) Let $x \in \langle a^l \rangle$. In that case, $x = \left(a^l\right)^r$ for some $r \in \mathbb{Z}$. We deduce that

$$x = \left(a^{qd}\right)^r = \left(a^d\right)^{qr} \in \left\langle a^d \right\rangle. \tag{28}$$

This shows that $\langle a^l \rangle \subseteq \langle a^d \rangle$.

($\supseteq$) Let $x \in \langle a^d \rangle$. This means that $x = \left(a^d\right)^r$ for some $r \in \mathbb{Z}$. By Bézout's lemma (Theorem 1.9), $\exists\, s, t \in \mathbb{Z}$ such that $ks + lt = d$. We deduce that

$$x = \left(a^d\right)^r = \left(a^{ks+lt}\right)^r = \left(a^{ks}a^{lt}\right)^r = \left(\left(a^k\right)^s\left(a^l\right)^t\right)^r. \tag{29}$$

However, $a^k = e$, where $e \in G$ is the identity element of G, since $k = |a|$. Thus,

$$x = \left(\left(a^k\right)^s\left(a^l\right)^t\right)^r = \left(e^s\left(a^l\right)^t\right)^r = \left(a^l\right)^{tr} \in \left\langle a^l \right\rangle. \tag{30}$$

This shows that $\langle a^d \rangle \subseteq \langle a^l \rangle$. $\square$

Proposition 2.63 *Let G be a group, and let $a \in G$. Suppose that $|a| = k$ for some $k \in \mathbb{Z}^+$. Given $l \in \mathbb{Z}^+$, $\left|a^l\right| = \frac{k}{\gcd(k,l)}$.*

Proof Define $d = \gcd(k, l)$, and let $k = qd$ for some $q \in \mathbb{Z}$.

We claim that $\left|a^d\right| = q$. First, we notice that

$$\left(a^d\right)^q = a^{qd} = a^k = e, \tag{31}$$

where $e \in G$ is the identity element of G. Therefore, $\left|a^d\right| \leq q$. Further, if $r \in \mathbb{Z}^+$ such that $r < q$, then $a^{rd} \neq e$, since $rd < qd = k = |a|$. Thus, $\left|a^d\right| = q$.

By Proposition 2.61, we know that $\left|a^l\right| = \left|\left\langle a^l \right\rangle\right|$. Now, by Proposition 2.62, $\langle a^l \rangle = \langle a^d \rangle$. Thus, $\left|a^l\right| = \left|\left\langle a^d \right\rangle\right| = \left|a^d\right| = q$, due to the claim. $\square$

Proposition 2.64 *Let G be a group. If H is a subgroup of G and K is a subgroup of H, then K is a subgroup of G.*

Proof Let $H \leq G$ and $K \leq H$. We will show that $K \leq G$. Let $a, b \in K$. In that case, since K is a group, $b^{-1} \in K$. Further, $ab^{-1} \in K$. Thus, by Proposition 2.57, $K \leq G$. $\square$

Proposition 2.65 *Let G be a group. The center $Z(G)$ is a subgroup of G.*

Proof Let $a, b \in Z(G)$. Given $x \in G$, we notice that $bx = xb$. Thus, $bxb^{-1} = x$, and so $xb^{-1} = b^{-1}x$. Further,

$$x\left(ab^{-1}\right) = axb^{-1} = ab^{-1}x = \left(ab^{-1}\right)x. \tag{32}$$

Now, by Proposition 2.57, we find that $Z(G)$ is a subgroup of G. $\square$

Proposition 2.66 *Let G be a group. Given $a \in G$, the centralizer $C(a)$ is a subgroup of G.*

Proof Let $a \in G$. We will show that $C(a)$ is a subgroup of G. Let $x, y \in C(a)$. In that case, $ax = xa$. Now, since $ay = ya$, we deduce that $y^{-1}ay = a$, and so $y^{-1}a = ay^{-1}$. Thus,

$$axy^{-1} = xay^{-1} = xy^{-1}a, \tag{33}$$

which shows that $xy^{-1} \in C(a)$. By Proposition 2.57, this shows that $C(a)$ is a subgroup of G. $\square$

Proposition 2.67 *Let $\sigma, \tau \in S_\Omega$. If σ and τ are disjoint cycles, then $\sigma \circ \tau = \tau \circ \sigma$.*

Proof Let $a \in \Omega$. Define $S = \left\{a \in \Omega \middle| \sigma(a) \neq a\right\}$ and $T = \left\{a \in \Omega \middle| \tau(a) \neq a\right\}$. As σ and τ are disjoint, we know that $S \cap T = \varnothing$. We consider three cases: $a \in S$, $a \in T$, or $a \notin S \cup T$.

Consider the case that $a \in S$. Suppose that $\sigma(a) = b$. We know that $a \neq b$, so since σ is bijective, $\sigma(b) \neq \sigma(a) = b$. Thus, $b \in S$. We deduce that $b \notin T$, so $\tau(b) = b$. Thus,

$$\tau\sigma(a) = \tau(b) = b = \sigma(a) = \sigma\tau(a). \tag{34}$$

Consider the case that $a \in T$. Suppose that $\tau(a) = c$. We know that $a \neq c$, so since τ is bijective, $\tau(c) \neq \tau(a) = c$. Thus, $c \in T$. We deduce that $c \notin S$, so $\sigma(c) = c$. Thus,

$$\tau\sigma\left(a\right) = \tau\left(a\right) = c = \sigma\left(c\right) = \sigma\tau\left(a\right). \tag{35}$$

Consider the case that $a \notin S \cup T$. This means that $\sigma(a) = a$ and $\tau(a) = a$. Therefore,

$$\tau\sigma\left(a\right) = \tau\left(a\right) = a = \sigma\left(a\right) = \sigma\tau\left(a\right). \tag{36}$$

Whatever the case, we see that $\tau\sigma(a) = \sigma\tau(a)$, and so $\tau\sigma = \sigma\tau$. $\square$

Proposition 2.68 *Let $\sigma \in S_n$ be a permutation. Suppose that $\sigma = \alpha_r \circ ... \circ \alpha_2 \circ \alpha_1$, where $\alpha_1, \alpha_2, ..., \alpha_r \in S_n$ are disjoint cycles and for each $i \in \{1, 2, ..., r\}$, the length of cycle α_i is k_i. In that case, $|\sigma| = \operatorname{lcm}\left(k_1, k_2, ..., k_r\right)$.*

Proof

Proposition 2.69 *Let G be a group. The quotient space ${}^{G}/_{H}$ is a group under coset multiplication if and only if $H \triangleleft G$.*

Proof

Proposition 2.70 *Let $\varphi : G_1 \to G_2$ be a homomorphism. Suppose that $e_1 \in G_1$ is the identity element of G_1 and $e_2 \in G_2$ is the identity element of G_2. In that case, $\varphi\left(e_1\right) = e_2$.*

Proof

Proposition 2.71 *Let $\varphi : G_1 \to G_2$ be a homomorphism. Given any element $a \in G_1$, $\varphi\left(a^{-1}\right) = \varphi\left(a\right)^{-1}$.*

Proof

Proposition 2.72 *Let* $\varphi : G_1 \to G_2$ *be a homomorphism. The map* φ *is a monomorphism if and only if* $\ker \varphi = \{e_1\}$*, where* $e_1 \in G_1$ *is the identity element of* G_1*.*

Proof

Proposition 2.73 *Let* $\varphi : G_1 \to G_2$ *be a group homomorphism. If* φ *is bijective, then* φ^{-1} *is also a group homomorphism.*

Proof

Proposition 2.74 *Let* $\varphi : G_1 \to G_2$ *be a homomorphism. In that case,* $\ker \varphi \triangleleft G_1$*.*

Proof

Proposition 2.75 *Let* G *be a group, and let* $N \triangleleft G$*. There exists a homomorphism* $\varphi : G \to {}^{G}/_{N}$ *such that* $\ker \varphi = N$*.*

Proof

2.3.1 Important theorems

Theorem 2.76 *Let G be a group, and let H be a subgroup of G. If G is cyclic, then H is cyclic.*

Proof Let G be a cyclic group, and let $H \leq G$. In that case, $\exists\ a \in G$ such that $G = \langle a \rangle$. If $H = \{e\}$, where $e \in G$ is the identity element of G, then H is cyclic. Assume, therefore, that $H \neq \{e\}$. We define

$$S = \left\{ n \in \mathbb{Z}^+ \middle| a^n \in H \right\}. \tag{37}$$

We claim that $S \neq \varnothing$. Since $H \neq \{e\}$, $\exists\ b \in H$ such that $b \neq e$. Now, since $H \subseteq G$, $b = a^t$ for some $t \in \mathbb{Z} \setminus \{0\}$. If $t > 0$, then $b \in S$. If $t < 0$, then we notice that $a^{-t} = b^{-1} \in H$, since H is a group. In that case, $b^{-1} \in S$. Either way, $S \neq \varnothing$.

By the well-ordering principle (Theorem 1.7), our claim implies that S contains a least element. Let $m \in S$ be the least element of S. In that case, $a^m \in H$, which indicates that $\langle a^m \rangle \subseteq H$.

We claim that $H \subseteq \langle a^m \rangle$. Let $b \in H$. Since $H \subseteq G$, $b = a^k$ for some $k \in \mathbb{Z}$. Now, by the division algorithm (Theorem 1.8), $\exists\ q, r \in \mathbb{Z}$ such that $k = qm + r$ and $0 \leq r < m$. We notice that

$$b = a^k = a^{qm+r} = a^{qm}a^r. \tag{38}$$

We deduce that $a^r = a^{-qm}b \in H$. However, m is the least positive integer such that $a^m \in H$, so if $a^r \in H$, then r cannot be a positive integer; $r = 0$. Thus, $b = a^{qm} = (a^m)^q \in \langle a^m \rangle$.

Our claim implies that $H = \langle a^m \rangle$, and so H is a cyclic group. $\square$

Theorem 2.77 *Let $\sigma \in S_n$. There exist disjoint cycles $\alpha_1, \alpha_2, ..., \alpha_r \in S_n$ such that $\sigma = \alpha_r \circ ... \circ \alpha_2 \circ \alpha_1$.*

Proof

Theorem 2.78 *Let $\sigma \in S_n$. If $n > 1$, then there exist 2-cycles $\tau_1, \tau_2, ..., \tau_s \in S_n$ such that $\sigma = \tau_s \circ ... \circ \tau_2 \circ \tau_1$.*

Proof

Theorem 2.79 *Let $n \in \mathbb{Z}$ such that $n > 1$. Given $\alpha_1, \alpha_2, ..., \alpha_r, \beta_1, \beta_2, ..., \beta_s \in S_n$ which are transpositions, if $\prod_{i=1}^{r} \alpha_i = \prod_{j=1}^{s} \beta_j$, then $r \equiv s \pmod 2$.*

Proof

The following is known as Lagrange's theorem.

Theorem 2.80 *Let G be a finite group. If H is a subgroup of G, then the order of H divides the order of G.*

Proof

The following is known as Cauchy's theorem.

Theorem 2.81 *Let G be a finite group. If $p \in \mathbb{Z}^+$ is a prime number and p divides the order $|G|$, then $\exists\, a \in G$ such that the order of a is p.*

Proof

The following is known as Cayley's theorem.

Theorem 2.82 *Let G be a group. There exists a subgroup H of the symmetric group S_G such that $G \simeq H$.*

Proof

3 Ring theory

3.1 Dictionary of terms and notations

Definition 3.1 *Let R be a nonempty set, and let $+$ and $\cdot$ be binary operations on R. We say that $(R, +, \cdot)$ is a ring provided that the following statements are true.*
(i) $(R, +)$ is an abelian group.
(ii) $\cdot$ is associative.
(iii) $\forall\, a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \tag{39}$$

and

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)\,. \tag{40}$$

Notation Given a ring R and $a, b \in R$, we will often denote $a \cdot b$ by "ab."

Definition 3.2 *Let $(R, +, \cdot)$ be a ring. The zero, or additive identity of R is the element $0 \in R$ such that $\forall\, a \in R$, $a + 0 = 0 + a = a$.*

Definition 3.3 *Let $(R, +, \cdot)$ be a ring. We say that R is a commutative ring provided that $\cdot$ is commutative.*

Definition 3.4 *Let $(R, +, \cdot)$ be a ring. A one, or multiplicative identity of R is an element $1 \in R$ such that $\forall\, a \in R$, $1a = a1 = a$.*

Definition 3.5 *Let R be a ring. We say that R is a ring with unity provided that there exists a multiplicative identity of R.*

Definition 3.6 *Let R be a ring with unity. Given $a, b \in R$, we say that b is a multiplicative inverse of a provided that $ab = ba = 1$.*

Definition 3.7 *Let R be a commutative ring with unity. A polynomial with coefficients in R is a sequence $(a_n)_{n=0}^{\infty}$ satisfying the following condition: $\exists\, n \in \mathbb{N}$ such that $\forall\, m \in \mathbb{N}$, if $m > n$, then $a_m = 0$.*

Definition 3.8 *Let R be a commutative ring with unity, and let $f = (a_n)_{n=0}^{\infty}$ be a nonzero polynomial with coefficients in R. The* <u>*degree of f*</u> *is the non-negative number* $\deg f = \max\left\{n \in \mathbb{N} \middle| a_n \neq 0\right\}$.

Definition 3.9 *Let R be a commutative ring with unity, and let $f = (a_n)_{n=0}^{\infty}$ be a polynomial with coefficients in R. The* <u>*leading coefficient of f*</u> *is the element $a_{\deg f}$.*

Definition 3.10 *Let R be a commutative ring with unity, and let $f = (a_n)_{n=0}^{\infty}$ be a polynomial with coefficients in R. We say that f is* <u>*monic*</u> *provided that the leading coefficient of f is* 1.

Definition 3.11 *Let R be a commutative ring with unity, and let $f = (a_n)_{n\in\mathbb{N}}$ be a polynomial with coefficients in R. We say that f is a* <u>*constant polynomial*</u> *provided that* $\forall\, n \in \mathbb{Z}^+$*,* $a_n = 0$*.*

Definition 3.12 *Let R be a commutative ring with unity. The* <u>*ring of polynomials with coefficients in R*</u> *is the ring $R[X]$ whose elements are the polynomials with coefficients in R and with $+$ defined via*

$$(a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty} = (a_n + b_n)_{n=0}^{\infty}$$

and with $\cdot$ defined via

$$(a_n)_{n=0}^{\infty} \cdot (b_n)_{n=0}^{\infty} = \left(\sum_{i+j=n} a_i b_j\right)_{n=0}^{\infty}.$$

Notation Given a commutative ring R with unity, we will often refer to the subring $\left\{(r, 0, 0, ...) \in R[X] \middle| r \in R\right\}$ of $R[X]$ as R.

Definition 3.13 *Let R be a commutative ring with unity. The* <u>*indeterminate over R*</u> *is the polynomial $X = (0, 1, 0, 0, ...)$.*

Notation Given a polynomial $f = (a_0, a_1, ..., a_n, 0, 0, ...)$, we will often write f as a linear combination of powers of the indeterminate: $a_n X^n + ... + a_1 X + a_0$. When doing so, we will write $f(X)$ instead of f.

Definition 3.14 *Let R be a commutative ring. Given $n \in \mathbb{Z}^+$, the matrix ring of degree n over R is the ring of $n \times n$ matrices over R.*

Definition 3.15 *Let D be a commutative ring with unity. We say that the ring D is an integral domain provided that $\forall\ a, b \in D$, if $ab = 0$, then $a = 0$ or $b = 0$.*

Definition 3.16 *Let D be an integral domain. Given $a, b \in D$, we say that a divides b, that a is a factor of b, or that b is divisible by a in D provided that $\exists\ q \in D$ such that $b = qa$.*

Definition 3.17 *Let $(R, +, \cdot)$ be a ring. Given a nonempty $S \subseteq R$, we say that S is a subring of R provided that $\forall\ a, b \in S$, $a + b, ab \in S$ and S is a ring under $+\big|_{S \times S}$ and $\cdot\big|_{S \times S}$.*

Definition 3.18 *Let R be a ring. Given a subring I of R, we say that I is a left ideal of R provided that $\forall\ r \in R$ and $\forall\ a \in I$, $ra \in I$.*

Definition 3.19 *Let R be a ring. Given a subring I of R, we say that I is a right ideal of R provided that $\forall\ r \in R$ and $\forall\ a \in I$, $ar \in I$.*

Definition 3.20 *Let R be a ring. Given a subring I of R, we say that I is a two-sided ideal of R provided that $\forall\ r \in R$ and $\forall\ a \in I$, $ra, ar \in I$.*

Notation If R is a commutative ring, then we will often write the statement "I is an ideal of R" as "$I \triangleleft R$."

Definition 3.21 *Let R be a commutative ring with unity. Given an ideal P of R, we say that P is a prime ideal of R provided that $\forall\ a, b \in R$, if $ab \in P$, then either $a \in P$ or $b \in P$.*

Definition 3.22 *Let R be a commutative ring. Given an ideal M of R, we say that M is a maximal ideal of R provided that $\forall\ I \triangleleft R$, if $M \subseteq I \subseteq R$, then $M = I$ or $I = R$.*

Definition 3.23 *Let R be a commutative ring, and let $S \subseteq R$ be a nonempty set. The ideal generated by S in R is the ideal $I \triangleleft R$ such that $S \subseteq I$ and, $\forall\ J \triangleleft R$, if $S \subseteq J$, then $I \subseteq J$.*

Notation Given a ring R and a nonempty $S \subseteq R$,

1. We will often denote the ideal generated by S by "(S)."

2. When $S = \{a_1, a_2, ..., a_n\}$, we may denote the ideal generated by S by "$(a_1, a_2, ..., a_n)$."

Definition 3.24 *Let R be a commutative ring, and let I be an ideal of R. We say that I is a principal ideal provided that $\exists\, a \in R$ such that $I = (a)$.*

3.2 Examples

Example 3.25 *The following are examples of rings.*

(i) $\mathbb{Z}$*, with its usual addition and multiplication.*

(ii) $\mathbb{Q}$, $\mathbb{R}$*, and* $\mathbb{C}$*, with their usual additions and multiplications, are all rings.*

(iii) $\{0\}$ *is a trivial ring.*

(iv) The rings above are all commutative. Given a ring R *and* $n \in \mathbb{Z}$ *such that* $n \geq 2$*, the matrix ring* $M_n(R)$ *is a non-commutative ring.*

3.3 Propositions, and their proofs

Proposition 3.26 *Let R be a ring. Given $a \in R$, $a0 = 0a = 0$.*

Proof

Proposition 3.27 *Let R be a ring with unity. Given $a, b \in R$, if a and b are both multiplicative identities of R, then $a = b$.*

Proof

Proposition 3.28 *Let R be a ring. Given $a, b, c \in R$, if $ab = 1$ and $ac = 1$, then $b = c$.*

Proof

Proposition 3.29 *Let R be a commutative ring. The ring R is an integral domain if and only if the following condition is true: $\forall\, a, b, c \in R$, if $ab = ac$, then $b = c$.*

Proof

3.3.1 Important theorems

4 Field theory

4.1 Dictionary of terms and notations

Definition 4.1 *Let K be a commutative ring with unity. We say that K is a field provided that $\forall\, a \in K$, $\exists\, b \in K$ such that $ab = 1$.*

4.2 Examples

4.3 Propositions, and their proofs

4.3.1 Important theorems