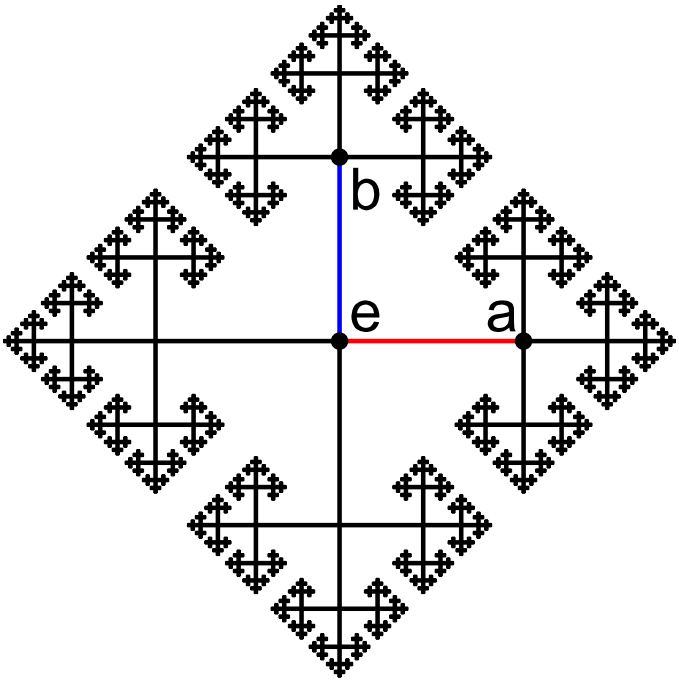
Introductory Group Theory



Parsiad Azimzadeh
http://parsiad.ca

These are some condensed notes that can be used to guide an introductory course on group theory. Enjoy!

Contents

1 *Introduction*

Definition 1 (Group)**.** A group $(G, *)$ consists of a set G and binary operation $* : G \times G \to G$ such that

1. for all a, b, c in G, $(a * b) * c = a * (b * c)$;
2. there exists e in G such that for all a in G, $a * e = e * a = a$;
3. for all a in G, there exists a' such that $a * a' = a' * a = e$.

In lieu of $a * b$, we often suppress $*$ and simply write ab. With an abuse of notation, we sometimes denote the group $(G, *)$ by G when the operation $*$ is understood. The element e in (2) is referred to as the *identity* of the group and a' in (3) is referred to as the *inverse* of a.

If condition (3) is omitted, we refer to the resulting structure as a *monoid*. When only (1) holds, we refer to the resulting structure as a *semigroup*.

When G is a finite set, we can represent it in a "*Cayley table*." For $G = \{+1, -1, +i, -i\}$ with the usual notion of multiplication in $\mathbb{C}$ restricted to G:

$\times$	$+1$	-1	$+i$	$-i$
$+1$	$+1$	-1	$+i$	$-i$
-1	-1	$+1$	$-i$	$+i$
$+i$	$+i$	$-i$	-1	$+1$
$-i$	$-i$	$+i$	$+1$	-1

Let F be a field (fields are defined in Definition 78; alternatively, for the time being, it is okay to think of a field as any one of $\mathbb{R}$, $\mathbb{Q}$, or $\mathbb{C}$ in examples). An important group is the *general linear group* of dimension n. This is the set

$$GL_n(F) = \{A \in F^{n \times n} : A \text{ is nonsingular}\}$$

with the usual notion of matrix multiplication. In general, the group operation is not commutative (when the group operation is commutative, the group is said to be *abelian*). The closure of this group with respect to multiplication follows directly from $\det AB = \det A \det B$ and $\det A \neq 0$ when A is nonsingular.

Lemma 2. *Suppose a, b, c in a group satisfy $ba = ca$ or $ab = ac$. Then, $b = c$.*

Proof. Right-multiply (resp. left-mult.) the equation by the inverse of a to get $b = c$. □

Theorem 3. *A group has unique inverses.*

Proof. Suppose an element a has inverses a' and a''. Then, $aa' = aa''$. It follows by the previous result that $a' = a''$. □

Since the inverse of an identity in a group is itself, it follows that:

Corollary 4. *A group has unique identity.*

We use the notations a' and a^{-1} interchangeably for the inverse of a along with

$$a^0 = e,\ a^n = \underbrace{aa \cdots a}_{n \text{ factors}}, \text{ and } a^{-n} = (a^{-1})^n.$$

Note that $a^{m+n} = a^m a^n$ and $(a^m)^n = a^{mn}$. However, $(ab)^n$ is not necessarily equal to $a^n b^n$, unless of course, the group is abelian.

Definition 5. The order of a group $(G, *)$ is the cardinality of G, denoted $|G|$.

Definition 6. The order of an element a in a group is $|a| = \inf\{n \geq 1 : a^n = e\}$.

2 *Subgroups and cyclic groups*

Definition 7. Let $(G, *)$ be a group. If $H \subset G$ and $(H, * \,|_H)$ is a group, we write $(H, * \,|_H) < (G, *)$.

Note that $\{e\}$ is always a subgroup of G, referred to as the trivial group. We interpret the symbol $\not<$ as "not a subgroup of." Some authors use $<$ to denote proper subgroup (we do not).

Lemma 8. *Let $(G, *)$ be a group and $H \subset G$. $(H, * \,|_H) < (G, *)$ if and only if*

1. *H is closed under $* \,|_H$;*
2. *e (the identity of G) is in H;*
3. *for all a in H, a^{-1} is in H.*

The *special linear group* is a subgroup of the general linear group whose elements have determinant one. That is,

$$SL_n(F) = \left\{ A \in F^{n \times n} : \det A = 1 \right\}.$$

Clearly, I is in $SL_n(F)$. Given two matrices A and B in $SL_n(F)$, since $\det AB = \det A \det B$, AB is in $SL_n(F)$. Given A in $SL_n(F)$, A^{-1} must be in $SL_n(F)$ since $\det A^{-1} = 1/\det A$.

We can, however, do better when it comes to subgroup testing:

Theorem 9 (One-step subgroup test)**.** *Let $(G, *)$ be a group and $\emptyset \neq H \subset G$. $(H, * \,|_H) < (G, *)$ if H is closed under division (i.e. if a, b are in H, so too is $a^{-1}b$).*

Proof. Since H is nonempty, there exists an element x in H. Therefore, $x^{-1}x = e$ is in H. It follows, that the inverse of any element x is also in H (take $a = x$, $b = e$). Closure under $*$ follows easily now (for x, y in H take $a = x^{-1}$ and $b = y$). □

Corollary 10 (Two-step subgroup test)**.** *Let $(G, *)$ be a group and $\emptyset \neq H \subset G$. $(H, * \mid_H) < (G, *)$ if H is closed under $*$ and for all a in H, a^{-1} is in H.*

Corollary 11 (Finite subgroup test)**.** *Let $(G, *)$ be a group and $\emptyset \neq H \subset G$ be a **finite** subset of G. $(H, * \mid_H) < (G, *)$ if H is closed under $*$.*

Proof. We need only show that for any a in H, a^{-1} is in H. If $a = e$, $a^{-1} = a$ is in H. Suppose then $a \neq e$ be in H. Closure implies a^n is in H for any $n \geq 0$. Finitude implies $a^i = a^j$ for some $i > j$, and hence $a^{i-j} = e$. Since $a \neq e$, $i - j > 1$, and we can write $aa^{i-j-1} = e$, and hence $a^{-1} = a^{i-j-1}$ is in H. □

Lemma 12. *Let $(G, *)$ be a group with some element a. Let $\langle a \rangle = \{a^n : n \text{ is an integer}\}$ (with the convention $a^0 = e$). Then, $(\langle a \rangle, * \mid_{\langle a \rangle}) < (G, *)$.*

We thus refer to $(\langle a \rangle, * \mid_{\langle a \rangle})$ as the cyclic subgroup generated by a (the "generator"). Trivially, all cyclic groups are abelian.

Definition 13 (Center)**.** The center of a group $(G, *)$ is

$$Z(G, *) = \{a \in G : \forall x \in G : ax = xa\}.$$

We sometimes write $Z(G)$ or Z when context permits.

Lemma 14. *For any group G, $Z(G) < G$.*

Proof. If a and b are in the center, so too must be ab since for any element x, $abx = axb = xab$. If a is in the center, then for any element x, $ax = xa$. Left and right multiplying by the inverse of a yields $a^{-1}axa^{-1} = xa^{-1} = a^{-1}x = a^{-1}xaa^{-1}$. Hence, so too must a^{-1} be in the center. □

Definition 15 (Centralizer)**.** The centralizer of a group $(G, *)$ with respect to a in G is

$$C(G, *, a) = \{g \in G : ga = ag\}.$$

We sometimes write $C(a)$ when the underlying group is clear. The following is proved similarly to Lemma 14.

Lemma 16. *For any group G and element a in G, $C(a) < G$.*

Theorem 17. *Let G be a group and $\langle a \rangle$ be a cyclic subgroup of G. If a has infinite order, all distinct powers of a are distinct elements. Otherwise, $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.*

Proof. Suppose $a^i = a^j$. Then, $a^{i-j} = e$. If a has infinite order, $i = j$. If a has order n, then $|i - j| \geq n$. Moreover, $i - j = kn$ since otherwise $a^m = e$ for some $m < n$. □

Corollary 18. *If $|a|$ is finite and $a^k = e$ for some integer k, $|a|$ divides k.*

Lemma 19. *Let $\langle a \rangle$ be a cyclic group of order n. Then $\langle a^k \rangle = \langle a \rangle$ if and only if* $\gcd(k, n) = 1$.

Proof. Suppose $\gcd(k, n) = 1$. Then, there exist integers u, v such that $ku + nv = 1$. Therefore, $a^1 = a^{ku+nv} = a^{ku}a^{nv} = a^{ku}$ and hence a is in $\langle a^k \rangle$, and hence so too is a^2, a^3, etc.. For the converse, suppose $\gcd(k, n) = d > 1$ so that $k = td$ and $n = sd$. Then $(a^k)^s = a^{tsd} = a^{tn} = e$. Therefore $|a^k| \leq s < n$. □

Therefore, if a cyclic group has order n, it has $\phi(n)$ generators, where ϕ is Euler's totient function.

Lemma 20. *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose $H < \langle a \rangle$ and $H \neq \{e\}$ (the claim is trivial if $H = \{e\}$). Therefore, a^t is in H for some $t > 0$. Let m be the least such positive integer. Clearly, $\langle a^m \rangle < H$. We would like to show that this holds with equality. To do so, we pick $b = a^k$ in H and show that it is in $\langle a^m \rangle$. By the minimality of m, we can write $k = mq + r$, where $0 \leq r < m$. It follows that $a^r = a^{-mq}a^k$. However, $a^{-mq} = (a^m)^{-q}$. Therefore, a^r is in H. Since $r < m$, r must be zero. Therefore, $a^k = a^{mq}$ is in $\langle a^m \rangle$. □

Theorem 21. *Let $\langle a \rangle$ be a cyclic group of order n. For each divisor k of n, this group has exactly one subgroup of order k, namely $\langle a^{n/k} \rangle$.*

3 *Permutation groups*

Definition 22. $\sigma : A \to A$ is a permutation of A if it is a bijection. A permutation group of a set A is a set of permutations of A that form a group under composition.

If A is finite, the symmetric group is that consisting of all possible permutations, of which there are $|A|!$ of. We denote the symmetric group by S_n, where n is the number of elements in the underlying set. Note that S_n is not abelian if $n \geq 3$.

Consider, two permutations of $\{1, \ldots, 5\}$:

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \text{ and } Q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

In this notation, the top row is the input, mapping to corresponding elements of the bottom row. Their composition is

$$QP = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

The convention used here is the usual right-to-left function composition convention. The permutation computed above is $x \mapsto Q(P(x))$. We also use "cycle notation":

$$P = (125)\,(34) \text{ and } Q = (13)\,(2)\,(45) \equiv (13)\,(45)$$

and $QP = (135)(246)$. For example, (15) is shorthand for

$$\begin{pmatrix} 1 & 5 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}.$$

Lemma 23 (Disjoint cycles commute)**.** *If the pair of cycles α and β have no entries in common, $\alpha\beta = \beta\alpha$.*

Corollary 24. *The order of a permutation written in disjoint cycle form is the least common multiple of the lengths of the cycles.*

A cycle of length 2 is called a transposition, as it exchanges two elements. Any permutation can be written as a product of transpositions. For example,

$$(12345) = (15)\,(14)\,(13)\,(12)\,.$$

Lemma 25. *If $e = \beta_1\beta_2\ldots\beta_r$ (the identity) where each β_i is a transposition, then r is even.*

Lemma 26. *If a permutation α can be expressed as a product of an even (resp. odd) number of transpositions, every decomposition of α can be expressed as a product of an even (resp. odd) number of transpositions.*

Proof. Suppose $\alpha = \beta_1\cdots\beta_r = \gamma_1\cdots\gamma_s$. Then, $e = \alpha\alpha^{-1} = \beta_1\cdots\beta_r(\gamma_1\cdots\gamma_s)^{-1} = \beta_1\cdots\beta_r\gamma_s\cdots\gamma_1$. By the previous lemma, $r+s$ must be even, and hence r and s must have the same parity. □

We thus refer to permutations as either even or odd.

Theorem 27. *The set A_n of even permutations in S_n is a subgroup of S_n.*

Proof. The product of two even permutations is an even permutation. The inverse of an even permutation is an even permutation. □

4 Homomorphisms

Definition 28. A map $\varphi : (G, *) \to (G', *')$ is a group homomorphism if $\varphi(a * b) = \varphi(a) *' \varphi(b)$ is in G' for all a, b in G. Furthermore, we define:

1. *monomorphism*: a group homomorphism that is injective;
2. *epimorphism*: a group homomorphism that is surjective;
3. *isomorphism*: a group homomorphism that is bijective (and hence both a monomorphism and epimorphism);
4. *endomorphism*: a group homomorphism in which the domain and codomain are the same;
5. *automorphism*: a bijective group homomorphism in which the domain and codomain are the same (and hence both an isomorphism and an endomorphism).

Any pair of groups have at least one homomorphism between them: the trivial group homomorphism $\varphi : G \to G'$ with $\varphi(g) = e'$. If two groups G and G' are isomorphic, we write $G \simeq G'$. A classic example of is

$$(\mathbb{R}, +) \simeq ((0, \infty), \cdot)$$

under any of the isomorphisms in the family $\{x \mapsto c^x\}_{c>0}$ (e.g. $\varphi(x) = e^x$).

Lemma 29. *If G and G' are epimorphic and G is abelian, so too is G'.*

Proof. Let $\varphi(a), \varphi(b)$ be two elements of G'. Since G is abelian, $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a)$. □

Definition 30. Let $\varphi : G \to G'$ be a group homomorphism. The kernel of φ is

$$\ker \varphi = \varphi^{-1}(\{e\}) = \left\{x \in G : \varphi(x) = e'\right\}.$$

As an example, let $\varphi : GL_n(F) \to (\mathbb{R} \setminus \{0\}, \cdot)$ with $\varphi(A) = \det A$. This is trivially a homomorphism, and $\ker \varphi = SL_n(F)$.

Theorem 31 (Properties of homomorphisms)**.** *Let φ be a group homomorphism from G to G'. Then,*

1. *if e is the identity of G, $\varphi(e)$ is the identity of G';*
2. *for all a in G, $\varphi(a^{-1}) = \varphi(a)^{-1}$;*
3. *if $H < G$ then $\varphi(H) < G'$;*
4. *if $K' < G'$, then $\varphi^{-1}(K') < G$;*
5. *if $H < G$ is cyclic (resp. abelian; resp. normal in G; see Definition 53), so too is $\varphi(H)$;*
6. *for each integer n and group element a in G, $\varphi(a^n) = (\varphi(a))^n$;*
7. *for any g in G with finite order, $|\varphi(g)|$ divides $|g|$;*
8. *for any g in G with $\varphi(g) = g'$, $\varphi^{-1}(g') = g \ker \varphi$;*
9. *if $H < G$ and $|H|$ finite, $|\varphi(H)|$ divides $|H|$.*
10. *if $K' \lhd G'$, then $\varphi^{-1}(K') \lhd G$ (see Definition 53);*
11. *if φ is onto and $\ker \varphi = \{e\}$, φ is an isomorphism from G to G'.*

Proof. Let a be an element of G. (1) $\varphi(a) = \varphi(ae) = \varphi(a)\varphi(e)$ and hence $e = \varphi(e)$ by left-multiplication by $\varphi(a)^{-1}$. (2) $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$ and the desired result follows by left-multiplication by $\varphi(a)^{-1}$. (3) and (4) follow from the group homomorphism property and preservation of inverses. (5)–(8) are trivial. (9) follows from (8). (10) is proved similar to (5). (11) follows from (8). □

From this, it follows that $\ker \varphi < G$ (moreover, $\ker \varphi \lhd G$; see Theorem 61).

Definition 32. Let H be a subgroup of G. The left coset of H in G with respect to some g in G is defined as

$$gH = \{gh\}_{h \in H}.$$

The right coset is defined similarly.

Theorem 33. *Let φ be a group homomorphism from G to G' and let $H = \ker \varphi$. Let g be an element of G. Then*

$$\varphi^{-1}(\varphi(\{g\})) = \{x \in G : \varphi(x) = \varphi(g)\} = gH = Hg.$$

Proof. First, note that

$$gH = g \ker \varphi = \{gh : \varphi(h) = e'\}.$$

Let $K = \varphi^{-1}(\varphi(\{g\}))$. If $x = gh$ is in gH, then $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$ (since $H = \ker \varphi$). Therefore, x is in K. Suppose now that x is in K so that $\varphi(x) = \varphi(g)$. Taking $g = x$ and $h = e$, we have $gh = x$ with $\varphi(h) = e'$. The proof for the right coset is the same. □

Corollary 34. *A group homomorphism φ is a monomorphism if and only if* $\ker \varphi = \{e\}$.

Proof. Let $H = \ker \varphi$. If φ is injective, then $H = \{e\}$ since $\varphi(e) = e'$ and if anything else mapped to the identity, this would contradict injectivity. The converse follows as a corollary to Theorem 33. □

Theorem 35 (Cayley's theorem)**.** *Any group is isomorphic to a group of permutations.*

Proof. For any g in G, define $T_g(x) = gx$ (check that T_g is a permutation of G). Let $G' = \{T_g : g \in G\}$. We first show that G' equipped with function composition is a group. The identity is T_e, since $T_g T_e = T_e T_g = T_g$. The operation is associative since function composition is associative. Furthermore, for any g, $T_{g^{-1}} T_g = T_g T_{g^{-1}} = T_e$ and hence G' contains its inverses.

Consider $\varphi : G \to G'$ with $\varphi(g) = T_g$. Note that $\varphi(ab) = T_{ab}$ and $\varphi(a)\varphi(b) = T_a T_b$ and $T_a(T_b(g)) = abg = T_{ab}(g)$, thereby satisfying the homomorphism property. Suppose now $\varphi(a) = \varphi(b)$. Then, $T_a = T_b$, or $ax = T_a(x) = T_b(x) = bx$ for all x, implying $a = b$. Surjectivity is trivial. □

The following gathers results that have previously been proven above, or are trivial:

Theorem 36 (Properties of isomorphisms)**.** *Let φ be a group isomorphism from G to G'. Then,*

1. *for all a, b in G, $ab = ba$ if and only if $\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$;*
2. *G is abelian if and only if G' is abelian;*
3. *for all a in G, $|a| = |\varphi(a)|$;*
4. *G is cyclic if and only if G' is cyclic;*
5. *for b in G, $x^k = b$ has the same number of solutions in G as $x^k = \varphi(b)$ in G' (k is an integer);*
6. *φ^{-1} is an isomorphism (from G' to G).*

Property (5) has some useful applications in showing that groups are not isomorphic. For example, consider $(\mathbb{C} \setminus \{0\}, \cdot)$ and $(\mathbb{R} \setminus \{0\}, \cdot)$. The equation $x^4 = 1$ has four solutions in the former, but only two in the latter (note that 1 is the identity in both, so that any isomorphism φ must satisfy $\varphi(1) = 1$).

Definition 37. Let G be a group with a in G. The function $\varphi_a(x) = axa^{-1}$ is called the inner automorphism of G induced by a.

It is easy to show that φ_a is an automorphism (it maps G to itself, it is bijective, and it satisfies the homomorphism property). We denote the set of automorphisms of G by $\mathrm{Aut}(G)$ and inner automorphisms of G by $\mathrm{Inn}(G)$.

Theorem 38. *Let G be a group.* $\mathrm{Aut}(G)$ *and* $\mathrm{Inn}(G)$ *equipped with function composition are both groups.*

Proof. Consider $\mathrm{Aut}(G)$. Denoting by φ and φ' two automorphisms, $\varphi \circ \varphi'$ is an automorphism. Furthermore, the identity mapping (i.e. $\psi(x) = x$) is an automorphism and serves as the identity for the group. For any automorphism φ, φ^{-1} is an automorphism and $\varphi \circ \varphi^{-1}$ is the identity.

Consider $\mathrm{Inn}(G)$. Denoting by φ_a and φ_b two inner automorphisms, $\varphi_a \circ \varphi_b$ is an inner automorphism since $\varphi_a(\varphi_b(x)) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x)$. The inner automorphism φ_e is the identity mapping and serves as the identity for the group. Lastly, it is easy to see that φ_a and $\varphi_{a^{-1}}$ are inverses for any inner automorphism φ_a. □

5 *Direct products*

Definition 39 (External direct product)**.** Let $G_1, \ldots, G_n$ be groups. The external direct product $G_1 \bigoplus \cdots \bigoplus G_n$ is the set of all n-tuples for which the i-th component is an element of G_i, and the operation is component-wise.

It is easy to see that this is a group with unity $(e_1, \ldots, e_n)$. Note that G_1, G_2, etc. are not subsets of the external direct product and therefore not subgroups of it either (hence "external").

Lemma 40. *Let $G = G_1 \oplus \cdots \oplus G_n$ be an external direct product of groups with $a = (a_1, \ldots, a_n)$ in G. Then, $|a| = \text{lcm}\{|a_1|, \ldots, |a_n|\}$.*

Proof. Let $k = \text{lcm}\{|a_1|, \ldots, |a_n|\}$. Clearly, $a^k = e$ since k divides $|a_i|$ for each i. Suppose that $|a| = j < k$. Then for all i, $a_i^j = e_i$ and hence $|a_i|$ divides j, a contradiction. □

Theorem 41. *Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.*

Proof. Let $G = \langle g \rangle$, $|G| = m$, $H = \langle h \rangle$, and $|H| = n$. Note that $|G \oplus H| = mn$.

Suppose m and n are relatively prime. Then (g, h) has order mn and hence $\langle (g, h) \rangle$ is cyclic.

Suppose m and n are not relatively prime. Let (g^k, h^j) be an element of $G \oplus H$. Since $\ell = \text{lcm}(m, n) < mn$ and $(g^k, h^j)^\ell = e$, every element of $G \oplus H$ has order lower than mn, and $G \oplus H$ is not cyclic. □

Corollary 42. *Let $G = G_1 \oplus \cdots \oplus G_n$ be an external direct product of finite cyclic groups. G is cyclic if and only if $|G_1|, \ldots, |G_n|$ are (pairwise) relatively prime.*

Corollary 43. *$\mathbb{Z}_{n_1 \cdots n_k} \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_k}$ if and only if $n_1, \ldots, n_k$ are relatively prime.*

Definition 44 (Internal direct product)**.** Let G be a group and $H_1, \ldots, H_n < G$. G is said to be the internal direct product of $H_1, \ldots, H_n$ if $\varphi : H_1 \oplus \cdots \oplus H_n \to G$ with $\varphi(h_1, \ldots, h_n) = \prod_{i=1}^{n} h_i$ is a group isomorphism.

A result relating external and internal direct products is given in Theorem 65.

6 Cosets and normal subgroups

Cosets are defined in Definition 32. We gather below some trivial properties of cosets:

Theorem 45. *Let H be a subgroup of G with a, b in G. Then,*

1. *a is in aH (resp. Ha);*
2. *$aH = H = Ha$ if and only if a is in H;*
3. *$aH = bH$ or $aH \cap bH = \emptyset$ (resp. $Ha = Hb$ or $Ha \cap Hb = \emptyset$);*
4. *$aH = bH$ (resp. $Ha = Hb$) if and only if $a^{-1}b$ (resp. ab^{-1}) is in H;*
5. *$|aH| = |bH| = |Ha| = |Hb|$;*
6. *$aH = Ha$ if and only if $a^{-1}Ha = H$;*
7. *aH (resp. Ha) is a subgroup of G if and only if a is in H.*

Proof. (1) H contains the identity and hence $ae \in aH$.

(2) If $a \in H$, we have $aH \subset H$ since $ah \in H$ for any $h \in H$. For an arbitrary $b \in H$, take $h = a^{-1}b$ to get $ah = b$ so that $aH \supset H$, and hence $aH = H$. For the converse, if a is not in H, $a \in aH$ and hence $aH \neq H$.

(3) Suppose $ah \in bH$ for some $h \in H$. Then, $a = bh'h^{-1}$ for some $h' \in H$ and hence $a \in bH$. Moreover, $ah'' = bh'h^{-1}h''$ for any $h'' \in H$ and hence $aH \subset bH$. Similarly, $bH \subset aH$, and hence $aH = bH$.

(4) Suppose $a^{-1}b \in H$. Then, $aa^{-1}bh = bh$ is in aH for any $h \in H$, and therefore $aH \supset bH$. Similarly, $b^{-1}a \in H$ since H is closed under inversion and hence $bH \supset aH$. For the converse, if $a^{-1}b \notin H$, then $b \notin aH$, but $b \in bH$.

(5) It's easy to see that $|aH| = |H|$ for any a.

(6) If $a^{-1}Ha = H$, any element of H can be written $a^{-1}ha$, where $h \in H$. Therefore, $aH = \{ah\}_{h\in H} = \{a(a^{-1}h'a)\}_{h'\in H} = Ha$. As for the converse, suppose $a^{-1}Ha \neq H$. Then, there exists $h \in H$ such that either (i) $a^{-1}ha \notin H$ or (ii) $h \notin a^{-1}Ha$. In case (i), $ha \neq ah'$ for all $h' \in H$. In case (ii), $ah \neq h'a$ for all $h' \in H$.

(7) If $a \in H$ it is easy to check that aH is a group. If aH is a group, then $e = ah$ for some h, and hence $h^{-1} = ahh^{-1} = a \in H$. □

In particular, (1) and (3) imply that left (resp. right) cosets partition G (i.e. there is a subset G' of G such that $G = \bigcup_{a\in G'} aH$ and $\{aH\}_{a\in G'}$ are pairwise disjoint).

Theorem 46 (Lagrange's theorem)**.** *If G is a finite group and $H < G$, then $|H|$ divides $|G|$. Moreover, the number of distinct left (resp. right) cosets of H in G is $|G|/|H|$.*

Proof. Denote by $\{a_iH\}_{i=1}^{r}$ the distinct left cosets of H in G. Since $G = \bigcup_{i=1}^{r} a_iH$ and distinct cosets are disjoint, $|G| = \sum_{i=1}^{r} |a_iH|$. Since $|a_iH| = |H|$, $|G| = r|H|$. □

$|G|/|H|$ is referred to as the index of H in G, and sometimes written $[G : H]$.

Corollary 47. *If G is a finite group and a is in G, $|a|$ divides $|G|$.*

Proof. Since $|a| = |\langle a\rangle|$ and $\langle a\rangle < G$ this follows from Lagrange's theorem. □

Corollary 48. *If G is a group of prime order, it is cyclic.*

Proof. Let $a \neq e$ be an element of G. Then $\langle a\rangle < G$. Furthermore, $|\langle a\rangle| > 1$ and $|\langle a\rangle|$ divides $|G|$. Since $|G|$ is a prime, it follows that $|\langle a\rangle| = |G|$ and hence $\langle a\rangle = G$. □

Corollary 49. *Let a be an element of a finite group G. Then, $a^{|G|} = e$.*

Proof. By Corollary 47, $a^{|G|} = a^{k|a|} = e$. □

We can now prove Euler's theorem. To do so, we first introduce a new group:

Definition 50 (Group of units in $\mathbb{Z}_n$)**.** Let n be a positive integer. Let U_n be the set of elements of $\mathbb{Z}_n = \{0, \ldots, n-1\}$ with inverses under multiplication modulo n.

Trivially, U_n is a group under multiplication modulo n.

Lemma 51. *$U_n = \{m \in \mathbb{Z}_n : m$ and n are coprime$\}$.*

Proof. This is a direct consequence of Bézout's lemma (i.e. $d = \gcd(m, n)$ is the smallest positive integer that can be written as $am = d + bn$ for integers a, b). □

Corollary 52 (Euler's theorem)**.** *Let a and n be coprime. Then, $a^{\phi(n)} \equiv 1 \mod n$, where ϕ is Euler's totient function.*

Proof. Lemma 51 establishes that $|U_n| = \phi(n)$. By Corollary 49, $a^{|U_n|} \equiv 1 \mod n$. □

Definition 53. Let G be a group and $H < G$. H is normal if $aH = Ha$ for all a in G.

We denote a normal subgroup with $H \lhd G$. Trivially, $Z(G) \lhd G$ (recall $Z(G)$ is the center of G). Some other examples of normal subgroups are $A_n \lhd S_n$ (recall A_n is the set of even permutations), $SL_n(F) \lhd GL_n(F)$.

Theorem 54 (Normal subgroup test)**.** *Let G be a group and $H < G$. $H \lhd G$ if and only if for all elements a in G, $a^{-1}Ha \subset H$.*

Proof. Suppose that for all $a \in G$, $a^{-1}Ha \subset H$ (and hence $aHa^{-1} \subset H$ as well). Let $a \in G$ and $h \in H$. Since $a^{-1}ha \in H$, Then, $a(a^{-1}ha) = ha$ and hence $aH \supset Ha$. Similarly, $Ha \supset aH$. As for the converse, suppose that $a^{-1}ha \notin H$. Then, $a(a^{-1}ha) = ha \notin aH$. □

As an application, we show (i) $A_n \lhd S_n$ and (ii) $SL_n(F) \lhd GL_n(F)$. (i) Let σ be a permutation in S_n. Then, for any even permutation σ', $\sigma^{-1}\sigma'\sigma$ is an even permutation, and hence $\sigma^{-1}A_n\sigma \subset A_n$. (ii) Let a be an element of $GL_n(F)$. Then $\det(a^{-1}ha) = \det(h)$, and hence $a^{-1}SL_n(F)a \subset SL_n(F)$.

Theorem 55. *Let G be a group and $H \lhd G$. The set $G/H = \{aH\}_{a \in G}$ is a group under the operation $(aH)(bH) = abH$.*

Proof. First, we must make sure that the group operation is well-defined. Suppose $aH = a'H$ and $bH = b'H$. By Theorem 45, $a'a^{-1} \in H$ and $b^{-1}b' \in H$. Therefore,

$$abH = Hab = \left\{ \left(ha'a^{-1} \right) ab \right\}_{h \in H} = Ha'b = a'bH$$
$$= \left\{ a'b \left(b^{-1}b'h \right) \right\}_{h \in H} = a'b'H.$$

The inverse of an element aH is $a^{-1}H$. □

The group G/H is called a quotient group or factor group.

With a slight abuse of notation, let $\mathbb{Z}$ be the group of integers under addition. An important family of quotient groups is $\{\mathbb{Z}/n\mathbb{Z}\}_{n>1}$ with

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

It is easy to show that $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$, the integers with addition modulo n.

Theorem 56. *Let G be a group. $G/Z(G)$ is cyclic if and only if G is abelian.*

Proof. By the hypothesis, $G/Z(G) = \langle gZ(G) \rangle$ for some g in G. Let a, b be elements of G with $aZ(G) = (gZ(G))^i = g^iZ(G)$ and $bZ(G) = g^jZ(G)$. Therefore, $a = g^ix$ and $b = g^jy$ for some x, y in $Z(G)$. Therefore,

$$ab = g^ixg^jy = xg^{i+j}y = xyg^{i+j} = yxg^{i+j} = yg^{i+j}x = g^jyg^ix = ba.$$

The converse is trivial: if G is abelian, $Z(G) = G$ and hence $G/Z(G) = G/G = \{aG\}_{a \in G}$. But, $aG = G$ independent of a, and hence $G/Z(G) = \{G\} = \langle G \rangle$. □

Recall that $\mathrm{Inn}(G) = \{x \mapsto a^{-1}xa : a \in G\}$ is the set of inner automorphisms.

Theorem 57. $G/Z(G) \simeq \mathrm{Inn}(G)$.

Proof. Let $\psi(aZ(G)) = \varphi_a$, where $\varphi_a(x) = axa^{-1}$.

We first show ψ is well-defined. If $aZ(G) = bZ(G)$, $a^{-1}b$ is in $Z(G)$ by Theorem 45. Therefore, for all x in G, $x = (a^{-1}b)^{-1}x(a^{-1}b) = b^{-1}axa^{-1}b$, or equivalently, $\varphi_a = \varphi_b$.

Clearly, ψ is surjective. If $\varphi_a = \varphi_b$, then for all x in G, $axa^{-1} = bxb^{-1}$, and hence $xa^{-1}b = a^{-1}bx$. That is, $a^{-1}b$ is in $Z(G)$, so that $aZ(G) = bZ(G)$. Lastly,

$$\psi((Z(G)a)(Z(G)b)) = \psi(Z(G)ab) = \varphi_{ab}$$
$$= \varphi_a \circ \varphi_b = \psi(Z(G)a)\psi(Z(G)b).$$

□

Definition 58 (Stabilizer of a point)**.** Let G be a group of permutations on a set S. Let s be an element of S. The stabilizer of s in G is

$$\operatorname{stab}_G(s) = \{\sigma \in G : \sigma(s) = s\}.$$

Definition 59 (Orbit of a point)**.** Let G be a group of permutations on a set S. Let s be an element of S. The orbit of $s$under G is

$$\operatorname{orb}_G(s) = \{\sigma(s) : \sigma \in G\} \subset S.$$

Theorem 60 (Orbit-stabilizer theorem)**.** *Let G be a subgroup of S_n, the symmetric group of order n. For any $1 \leq i \leq n$, $|G| = |\operatorname{stab}_G(i)||\operatorname{orb}_G(i)|$.*

Proof. Note that $H = \operatorname{stab}_G(i) \lhd G$ since for any σ in G, $\sigma^{-1}H\sigma \subset H$. Therefore, we can consider the quotient group $G/H = \{\sigma H\}_{\sigma \in G}$. To show $[G : H] = |G|/|H|$, it is sufficient to show that there exists a bijection between G/H and $\operatorname{orb}_G(i)$. Let $\varphi : G/H \to \operatorname{orb}_G(i)$ with $\varphi(\sigma H) = \sigma(i)$. First, we check that this function is well-defined. Let $\sigma, \sigma' \in G$ with $\sigma H = \sigma' H$, so that $\sigma^{-1}\sigma' \in H$, which implies $\sigma(i) = \sigma'(i)$. Similarly, φ is injective. φ is trivially surjective. □

Theorem 61 (First isomorphism theorem)**.** *Let $\varphi : G \to G'$ be a group homomorphism. Then,* $\ker\varphi \lhd G$ *and* $\varphi(G) \simeq G/\ker\varphi$.

Proof. The first part of the proof is trivial: $K = \ker\varphi < G$ and for any a in G, $a^{-1}Ka \subset K$ since $\varphi(a^{-1}xa) = \varphi(a)^{-1}\varphi(x)\varphi(a) = e'$ for x in K.

Since $K \lhd G$, G/K is well-defined. Let $\psi : G/K \to \varphi(G)$ with $\psi(xK) = \varphi(x)$. We first check ψ is well-defined. Let x and y be elements of G. Note that $xK = yK$ implies $x^{-1}y$ is in K, and hence $\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y) = e'$, or equivalently,

$\varphi(x) = \varphi(y)$. The converse is also true, so that ψ is injective. Trivially, ψ is surjective. Lastly, we check the homomorphism property:

$$\psi((xK)(yK)) = \psi(xyK) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(xK)\psi(yK).$$

□

As a simple example, consider the map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ with $\varphi(an + r) \equiv r \mod n$, where $0 \leq r < n$. It follows that $\ker \varphi = \langle n \rangle = n\mathbb{Z}$, so that $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Definition 62 (Normalizer)**.** The normalizer of a subgroup $(H, * \,|_G)$ of $(G, *)$ is

$$N(H, G, *) = \left\{ g \in G : g^{-1}Hg = H \right\}$$

wbere $g^{-1}Hg = \{ghg : h \in H\}$.

We sometimes write $N(H)$ when the underlying group is clear.

Theorem 63. *For any $H < G$, $N(H)/C(H) \simeq K$ where $K < \mathrm{Aut}(H)$.*

Proof. We first show $C(H)$ is normal so that $N(H)/C(H)$ is well-defined. To do so, we show that $y^{-1}C(H)y \subset C(H)$ for any y in G. Note that an element of $y^{-1}C(H)y$ is of the form $y^{-1}xy$ where x is in the centralizer. Furthermore, $(y^{-1}xy)^{-1}h(y^{-1}xy) = y^{-1}x^{-1}(yhy^{-1})xy = y^{-1}yhy^{-1}y = h$, as desired.

Let $\varphi : N(H) \to \mathrm{Aut}(H)$ with $\varphi(g) = \varphi_g$ the inner automorphism with respect to g. φ is a group homomorphism (check). It is easy to check that $\ker \varphi = C(H)$. The desired result follows from the first isormorphism theorem. □

Theorem 64. *If $N \lhd G$, there exists a homomorphism of which N is the kernel.*

Proof. Take $\varphi : G \to G/N$ with $\varphi(g) = gN$. It is easy to check that φ is a homomorphism. Furthermore, $\ker \varphi = \{g \in G : \varphi(g) = N\} = N$ since $gN = N$ if and only if g is in N. □

Theorem 65. *Let G be a group and $H_1, \ldots, H_n \leq G$. Then G is an internal direct product of $H_1, \ldots, H_n$ if and only if*

1. $G = \prod_{i=1}^{n} H_i = \{\prod_{i=1}^{n} h_i : h_i \in H_i\}$;
2. $H_i \cap H_j = \{e\}$ *for any* $i \neq j$;
3. $H_i \lhd G$ *for any* i.

Proof. It is sufficient to prove the case of $n = 2$. Let $\varphi(h_1, h_2) = h_1 h_2$.

Let h be in H_1 and H_2. Since φ is injective, we have $\varphi(h, h) = h^2 = \varphi(h^2, e)$. Therefore, h must be the identity, and hence $H_1 \cap H_2 = \{e\}$.

Since φ is surjective, the image $\varphi(H_1 \times H_2) = H_1 H_2 = G$.

By the homomorphism property, $\varphi((h_1, h_2)(k_1, k_2)) = \varphi(h_1 k_1, h_2, k_2) = h_1 k_1 h_2 k_2$ and $\varphi((h_1, h_2)(k_1, k_2)) = \varphi(h_1, h_2)\varphi(k_1, k_2) = h_1 h_2 k_1 k_2$ so that $k_1 h_2 = h_2 k_1$. Since k_1 and h_2 are arbitrary, we conclude that every element of H_1 commutes with every element of H_2. From this, it follows that $g^{-1} H_1 g = H_1$ and $g^{-1} H_2 g = H_2$ for any element g, and hence $H_1 \lhd G$ and $H_2 \lhd G$.

The converses of the above statements are similar in nature. □

Lemma 66. *Let G be a finite abelian group and p a prime such that $|G| = mp^n$ where p does not divide m. Then, $G = H \oplus K$ where $H = \{x \in G : x^{p^n} = e\}$ and $K = \{x \in G : x^m = e\}$.*

Proof. Note that K is a group since it is closed under inverse and if x and y are in K, $(xy)^m = x^m y^m = e$ (G is abelian). The same statement can be made of H. Moreover, this implies $H, K \lhd G$ since any subgroup of an abelian group is normal in that group.

By Theorem 65, it is sufficient to show $G = HK$ and $H \cap K = \{e\}$.

Since m and p^n are coprime, Bézout's Lemma yields the existence of integers s and t with $1 = sm + tp^n$. Therefore, $x = x^{sm+tp^n} = x^{sm} x^{tp^n}$. Since $x^{|G|} = x^{mp^n} = e$, $(x^{sm})^{p^n} = (x^{mp^n})^s = e^s = e$, and hence x^{sm} is in H. Similarly, x^{tp^n} is in K. Therefore, $G = HK$.

Suppose x is in both H and K. Therefore, $x^{p^n} = e = x^m$, or $x^{p^n - m} = e$. Therefore, $|x|$ divides p^n and m. Since these are coprime, $|x| = 1$, and hence $x = e$. □

Corollary 67 (Fundamental theorem of finite abelian groups)**.** *Let G be a finite abelian group. Let $\prod_{i=1}^{k} p_i^{n_i}$ be the prime factorization of $|G|$. Then $G = H_1 \oplus \cdots \oplus H_k$ where*

$$H_i = \left\{ x \in G : x^{p_i^{n_i}} = e_i \right\}.$$

The factorization of G is unique up to ordering of the factors.

7 *Rings and fields*

A ring is a set equipped with two operations that are related:

Definition 68. A ring $(R, +, *)$ consists of a set R and two binary operations $+, * : R \to R$ such that

1. $(R, +)$ is an abelian group;
2. $(R, *)$ is a semigroup;
3. for all a, b, c in R, $a(b + c) = (ab) + (ac)$ and $(a + b)c = (ac) + (bc)$.

When parentheses are omitted, multiplication $*$ takes precedence over addition $+$. A ring $(R, +, *)$ is said to be commutative if $(R, *)$ is abelian. We often refer to the identity in $(R, +)$ as 0 and that in $(R, *)$ as 1. As usual, we often omit $+$ and $*$ when they are understood and simply write R.

Some authors instead take instead (2) to be $(R, *)$ is a monoid. We refer to this as a *ring with unity* (a.k.a. unital ring, unitary ring, etc.). These authors refer to our definition as an *rng* or *pseudoring.*

Theorem 69 (Properties of rings)**.** *Let R be a ring with elements a, b, c. Then,*

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $a(b - c) = ab - ac$ *and* $(b - c)a = ba - ca$;
5. *If R is a ring with unity,* $(-1)a = -a$;
6. *If R is a ring with unity,* $(-1)(-1) = 1$.

Proof. (1) $a0 = a(0+0) = a0 + a0$ and hence $0 = a0$.
(2) $ab + a(-b) = a(b-b) = 0$ and hence $a(-b) = -(ab)$.
(3) $0 = (-a)(b-b) = -(ab) + (-a)(-b)$ and hence $ab = (-a)(-b)$.
The remaining claims follow. □

Theorem 70. *The additive and multiplicative identities in a ring are unique.*

Proof. Identical to the proof of Theorem 3. □

Corollary 71. *A ring has unique additive and multiplicative inverses.*

Note that the above claims concern uniqueness, not existence.

Definition 72 (Subring)**.** $(S, + \mid_S, * \mid_S)$ is a subring of a ring $(R, +, *)$ if $S \subset R$ and $(S, + \mid_S, * \mid_S)$ is itself a ring.

Theorem 73 (Subring test)**.** *S is a subring of a ring R if S is closed under subtraction and multiplication.*

Proof. Since $S$is closed under subtraction, $0 - a = -a$ is in S for each a in S, and hence S contains its additive inverses. Furthermore, it is closed under addition since $a + b = a - (-b)$ for a, b in S. □

Definition 74 (Zero divisor)**.** An element a of a commutative ring R is called a zero divisor if there exists x in R such that $ax = 0$.

Definition 75 (Integral domain)**.** A commutative ring R with unity is said to be an integral domain if it has no zero divisors.

Theorem 76. *If a, b, c are elements of an integral domain and $ab = ac$, $a = 0$ or $b = c$.*

Proof. $ab = ac$ can be written $a(b-c) = 0$. The result follows. □

Definition 77 (Unit)**.** An element of a ring is called a unit if it has a multiplicative inverse.

Definition 78 (Field)**.** A field is a commutative ring with unity in which every nonzero element is a unit.

Theorem 79. *D is a finite field if and only if D is a finite integral domain.*

Proof. If D is a finite field, it is trivially a finite integral domain.

Let D be an integral domain. If D is the trivial ring $\{0\}$ (with $0 = 1$), the claim is vacuously true. Otherwise, suppose a is a nonzero element of D. If $a = 1$, a is trivially a unit. If $a \neq 1$, consider $\langle a \rangle$ as a subgroup of $(D, *)$. Since D is finite, we must have $a^i = a^j$ for some $i > j$, and hence $a^j(a^{i-j} - 1) = 0$. By the assumption, either $a = 0$, or $a^{i-j} = 1$. Therefore, $a^{i-j-1}a = 1$, and hence a is a unit. □

Theorem 80. *$\mathbb{Z}_n$ is a field if and only if n is a prime.*

Proof. If $n = ab$ for $1 < a, b < n$, then $ab \equiv 0 \mod n$ and hence $\mathbb{Z}_n$ is not an integral domain. The other direction follows since Euler's theorem guarantees an inverse for each nonzero element. □

Definition 81 (Characteristic of a ring)**.** The characteristic of a ring R, $\text{char}(R)$, is the least positive integer n such that $\underbrace{x + \cdots + x}_{n \text{ times}} = 0$ for all x in R. If no such n exists, $\text{char}(R) = 0$.

Theorem 82. *Let R be a ring with unity and n a positive integer. $|1| = n$ in $(R, +)$ if and only if* $\text{char}(R) = n$.

Proof. If $|1| = n$, $\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$ so that $a + \cdots + a = a(1 + \cdots + 1) = a0 = 0$. Therefore, $\text{char}(R) = n$. The converse is trivial. □

Theorem 83. *The characteristic of an integral domain is either zero or prime.*

Proof. Suppose the characteristic is $n = st$. Then $\underbrace{1 + \cdots + 1}_{n \text{ times}} = (\underbrace{1 + \cdots + 1}_{s \text{ times}})(\underbrace{1 + \cdots + 1}_{t \text{ times}})$. Then, either $\underbrace{1 + \cdots + 1}_{s \text{ times}}$ or $\underbrace{1 + \cdots + 1}_{t \text{ times}}$ is zero, and hence one of s or t must be one. □

Definition 84 (Ideal)**.** A subring A of a ring R is called a (two-sided) ideal of R if for every r in R and every a in A, ra and ar are in A.

Theorem 85 (Ideal test)**.** *A nonempty subset of a ring R is an ideal of R if*

1. *$a - b$ is in A for all a, b in A;*

2. *ra or ar are in A for all a in A and r in R.*

$\{0\}$ is an ideal of any ring and hence referred to as the *trivial ideal*. Given an element a in a ring R, $\langle a \rangle = \{ar : r \in R\}$ is the *principal ideal* generated by a. This should not be confused with the notation of a cyclic group.

Since $(R, +)$ is an abelian group and any subring $(A, +)$ satisfies $(A, +) \lhd (R, +)$, we can form the quotient group $R/A : (R, +)/(A, +) = \{r + A : r \in R\}$ where $r + A = A + r = \{r + a : a \in A\}$. We might ask, is the resulting structure a ring?

Theorem 86. *Let R be a ring and A a subring of R. $(R, +)/(A, +)$ is a ring under the operations*

$$(s + A) + (t + A) = s + t + A$$
$$(s + A)(t + A) = st + A$$

if and only if A is an ideal of R.

The above and some of the following theorems are given without proof as they are similar to their group analogues.

Definition 87 (Prime ideal)**.** A proper ideal $A \subsetneq R$ of a ring R is a prime ideal if for any a and b in R, ab in A implies a and b are in A.

For example, in the ring $(\mathbb{Z}, +, *)$, $n\mathbb{Z}$ is a prime ideal if and only if n is a prime.

Another example is that $\langle x^2 + 1 \rangle$ is not a prime ideal in $\mathbb{Z}_2[x]$ (see Definition 100). To see this, note that $(x + 1)^2 = x^2 + 2x + 1 \equiv x^2 + 1 \mod 2$. However, $x \mapsto x + 1$ is not in $\langle x^2 + 1 \rangle$.

Definition 88 (Maximal ideal)**.** A proper ideal $A \subsetneq R$ of a ring R is said to be a maximal ideal if whenever B is an ideal of R and $A \subset B \subset R$, then $B = A$ or $B = R$.

Theorem 89. *Let R be a ring. R/A is an integral domain if and only if A is a prime ideal.*

Theorem 90. *Let R be a commutative ring with unity and A be an ideal of R. R/A is a field if and only if A is maximal.*

Definition 91. A ring homomorphism $\varphi : R \to R'$ from a ring R to a ring R' satisfies $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all a, b in R. A ring homomorphism that is bijective is called a ring isomorphism.

Theorem 92 (Properties of ring homomorphisms)**.** *Let $\varphi : R \to R'$ be a ring homomorphism, A be a subring of R and B an ideal of S. Then,*

1. *for all rin R, $\varphi(r + \ldots + r) = \varphi(r) + \ldots + \varphi(r)$;*
2. *$\varphi(A)$ is a subring of R';*
3. *if A is an ideal and φ is a surjective, $\varphi(A)$ is an ideal;*
4. *$\varphi^{-1}(B)$ is an ideal of R;*
5. *if R is commutative, $\varphi(R)$ is so too;*
6. *if R is a ring with unity, $R' \neq \{0\}$, and φ is surjective, then $\varphi(1)$ is the unity of R';*
7. *φ is an isomorphism if and only if φ is surjective and $\ker \varphi = \{0\}$;*
8. *if φ is an isomorphism, φ^{-1} is an isomorphism from R' to R.*

Theorem 93 (First isomorphism theorem for rings)**.** *Let $\varphi : R \to R'$ be a ring homomorphism. Then,*

1. *$\ker \varphi$ is an ideal of R;*
2. *$R/\ker \varphi \simeq \varphi(R)$ with isomorphism $r + \ker \varphi \mapsto \varphi(r)$.*

Theorem 94. *An ideal A of a ring R is the kernel of the homomorphism $r \mapsto r + A$.*

Lemma 95. *Let R be a ring with unity 1. The mapping $\varphi : \mathbb{Z} \to R$ given by*

$$n \mapsto \operatorname{sign}(n)(\underbrace{1 + \ldots + 1}_{|n| \text{ times}})$$

is a ring homomorphism.

Corollary 96. *A ring with unity contains a subring isomorphic to $\mathbb{Z}_n$ if it has characteristic $n > 0$ and contains a subring isomorphic to $\mathbb{Z}$ otherwise.*

Corollary 97. *$x \mapsto x \mod n$ is a ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$.*

Recall that the characteristic of an integral domain is either zero or prime.

Corollary 98. *A field contains a subfield isomorphic to $\mathbb{Z}_p$ if it has characteristic $p > 0$ and contains a subfield isomorphic to $\mathbb{Q}$ otherwise.*

Theorem 99 (Field of quotients)**.** *Let D be an integral domain. There exists a field that contains a subring isomorphic to D.*

The construction here is the usual construction of the rational numbers from the integers. We equip $D \times D$ with the equivalence relation $(a, b) \sim (c, d)$ whenever $ad = bc$. It can be shown that the set of resulting equivalence classes along with the operations $(a, b) + (c, d) = (ad + bc, bd)$ and $(a, b)(c, d) = (ac, bd)$ are a field. The subfield $\{[(a, 1)] : a \in D\}$ is isomorphic to D.

Definition 100 (Polynomial ring)**.** Let R be a commutative ring. The ring of polynomials over R is

$$R[x] = \left\{ \sum_{k=0}^{n} a_k x^k : n \text{ is a positive integer and } a_i \in \mathbb{R} \right\}$$

with the usual notions of addition and multiplication of polynomials.

Two elements $f(x) = \sum a_k x^k$ and $g(x) = \sum b_k x^k$ of $R[x]$ are equal when $a_k = b_k$ for all k. This means that even if $f(x) = g(x)$ for all x, f is not necessarily equal to g. Under this notion of equivalence, $R[x]$ is simply the subset of all sequences in $R^{\mathbb{N}}$ with finitely many nonzero terms.

Instead of saying f is in $R[x]$, we often say f is a polynomial over R.

Definition 101 (Degree)**.** The degree of a polynomial f over a ring R is

$$\deg f = \sup \{k \geq 0 : a_k \neq 0\}.$$

A polynomial is said to be monic if $a_{\deg f} = 1$.

According to the definition above, the degree of the zero polynomial is $\deg 0 = \sup \emptyset = -\infty$. Some authors use -1.

Theorem 102. *Let D be an integral domain and f, g be polynomials over D. Then,* $\deg(fg) = \deg f + \deg g$.

Proof. If $f(x) = \sum a_i x^i$ and $g(x) = \sum b_i x^i$ are polynomials of degree n and m, respectively, the coefficient of x^{n+m} in fg is $a_n b_m \neq 0$. □

Corollary 103. *If D is an integral domain, so too is $D[x]$.*

Theorem 104 (Division algorithm)**.** *Let F be a field and f, d be polynomials over F with $d \neq 0$. There exist q, r in $F[x]$ such that*

$$f = dq + r \text{ where } \deg r < \deg d.$$

Proof. If $\deg f < \deg d$, the result is trivial.

Otherwise, let $f(x) = \sum_{i=1}^{m} a_i x^i$ and $d(x) = \sum_{j=1}^{n} b_j x^j$. Let $p(x) = f(x) - d(x)\frac{a_m}{b_n} x^{m-n}$, eliminating the highest order term in f. Note that $\deg p < \deg f$. Continue this process until the resulting polynomial has degree less than that of d so that $f(x) - d(x)(\frac{a_m}{b_n} x^{m-n} + \cdots) = r(x)$. □

Corollary 105. *Let F be a field, a an element of F, and f a polynomial over F. Then, $f(a)$ is the remainder in the division of f by $x \mapsto x - a$.*

Corollary 106. *Let F be a field, a an element of F, and f a polynomial over F. Then, a is zero of f if and only if $x \mapsto x - a$ is a factor of f.*

Corollary 107. *Let F be a field and f a nonzero polynomial over F whose distinct zeros are $a_1, \ldots, a_k$ of multiplicities $n_1, \ldots, n_k$. f has the factorization*

$$f(x) = (x - a_1)^{n_1} \cdots (x - a_k)^{n_k} q(x)$$
$$\text{where } q \in F[x] \text{ and } \deg q < \sum_i n_i \leq \deg f.$$

Definition 108 (Principal ideal domain)**.** A principal ideal domain (PID) is an integral domain R in which every ideal has the form

$$\langle a \rangle = \{ra : r \in R\} \text{ for some } a \in R.$$

Theorem 109. *Let F be a field. Then, $F[x]$ is a PID.*

Let A be an ideal of $F[x]$. If $A = \{0\}$, then $A = \langle 0 \rangle$. Suppose therefore, that A has a nonzero element. Let g be a minimal degree polynomial in A. Suppose there exists f in A but not in $\langle g \rangle$. Then, $f = gq + r$ where r is nonzero and $\deg r < \deg g$. Then, $r = f - gq$, and is in A. However,

$$\begin{aligned}\deg r \geq \max\{\deg f, \deg gq\} &= \max\{\deg f, \deg g + \deg q\} \\ &= \deg g + \deg q \geq \deg g,\end{aligned}$$

a contradiction.

Corollary 110. *Let F be a field. Any nontrivial ideal A of $F[x]$ is of the form $\langle g \rangle$ where g is in $F[x]$. Furthermore, g has minimum degree in A.*

Definition 111 (Irreducible polynomial)**.** Let D be an integral domain. Let f be a nonzero polynomial that is not a unit in $D[x]$. f is said to be reducible over D if there exist g, h in $D[x]$ such that $f = gh$ and g and h that are not units in $D[x]$. Otherwise, f is said to be irreducible.

For example, $2x$ is irreducible over $\mathbb{Z}$. However, since 2 is a unit in $\mathbb{Q}$, $2x$ is reducible over $\mathbb{Q}$.

Theorem 112 (Reducibility test)**.** *Let F be a field. If f is a polynomial over F and $2 \leq \deg f \leq 3$ then f is reducible over F if and only if f has a zero in F.*

Proof. Suppose $f = gh$ with g and h nonconstant. Then $\deg f = 3 = \deg g + \deg h$ so that $\deg g = 1$ (w.l.o.g.). Then, $g(x) = ax + b$ so that $x = -a^{-1}b$ is a root of g, and hence a root of f. The converse is trivial. □

Definition 113 (Content of a polynomial)**.** The content of a polynomial $p(x) = \sum_{k=1}^{n} a_k x^k$ with integer coefficients is

$$c(p) = \gcd(a_0, \ldots, a_n)$$

where $\gcd(0, n) = n$. A primitive polynomial has content 1.

Theorem 114 (Gauss' lemma)**.** *If f, g are polynomials over $\mathbb{Z}$, $c(fg) = c(f)c(g)$.*

Proof. Since $c(f)c(g)$ is a common divisor of the coefficients of fg, it is sufficient to prove $c(fg) = 1$ whenever f and g are primitive.

Let $f = \sum a_k x^k$ and $g = \sum b_k x^k$ be primitive and suppose fg is not. Then there exists a prime p such that p is a common factor of the coefficients of fg. Let $r = \sup\{k \geq 0 : p \text{ does not divide } a_k\}$ and $s = \sup\{k \geq 0 : p \text{ does not divide } b_k\}$. Consider the coefficient of x^{r+s}: $\sum a_k b_{r+s-k}$. This sum contains $a_r b_s$, but all remaining terms $a_k b_{r+s-k}$ divisible by p since either $k > r$ or $k < r$ and hence $r + s - k < s$. We arrive at a contradiction. □

More generally, Gauss' lemma holds on any GCD domain. We do not consider GCD domains here.

Theorem 115. *Let f be a polynomial over $\mathbb{Z}$. If f is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$. Moreover, f has a factorization gh with $\deg g, \deg h \geq 1$.*

Proof. Let f be a polynomial over $\mathbb{Z}$ that is reducible over $\mathbb{Q}$. Then, $f = gh$ where g, h are nonunit polynomials over $\mathbb{Q}$. W.l.o.g., we take $c(f) = 1$ since otherwise, we could instead consider the polynomial $f/c(f)$. Let ℓ_g be the least common multiple of the denominators of the coefficients of g and define ℓ_h similarly. Then, $\ell_g g$ and $\ell_h h$ are polynomials over $\mathbb{Z}$. Let c_g be the content of $\ell_g g$ and define c_h similarly. Then, $\ell_g g = c_g g'$ and $\ell_h h = c_h h'$ for some primitive polynomials g', h' over $\mathbb{Z}$. Therefore, $\ell_g \ell_h = c(\ell_g \ell_h f) = c(c_g c_h g' h') = c_g c_h$ and hence $f = g'h'$. □

The contrapositive is also useful, as seen below:

Theorem 116 (Modulo p irreducibility test)**.** *Let p be a prime and f a polynomial over $\mathbb{Z}$ with degree greater or equal to 1. Let $\overline{f}$ be the polynomial obtained by replacing the coefficients of f with their least positive residues modulo p. If $\overline{f}$ is irreducible over $\mathbb{Z}_p$ and $\deg \overline{f} = \deg f$, f is irreducible over $\mathbb{Q}$.*

Proof. Suppose f is reducible over $\mathbb{Q}$. By Theorem 115, $f = gh$ where g, h are nonunit polynomials over $\mathbb{Z}$. Denote by $\overline{g}$ and $\overline{h}$ the respective polynomials reduced modulo p so that $\overline{f} = \overline{g}\overline{h}$.

Suppose $\deg \overline{g} \neq \deg g$ and $\deg \overline{h} \neq h$. Then,

$$\deg \overline{f} = \deg \overline{g}\overline{h} = \deg \overline{g} + \deg \overline{h} < \deg g + \deg h = \deg gh = \deg f.$$

It follows that $\overline{g}$ and $\overline{h}$ are nonunit polynomials over $\mathbb{Z}_p$ that factor $\overline{f}$. □

Note that we use a prime number p in the above since $\mathbb{Z}_n$ is not an integral domain for composite n.

Theorem 117 (Eisenstein's criterion)**.** *Let $f(x) = \sum_{k=0}^{n} a_k x^k$ be a polynomial over $\mathbb{Z}$. If there is a prime p such that p does not divide a_n, p divides a_k for $k < n$, and p^2 does not divide a_0, f is irreducible over $\mathbb{Q}$.*

Proof. We prove the contrapositive. Suppose f is reducible over $\mathbb{Q}$ and that there exists a p satisfying the above requirements. By Theorem 115, $f = gh$ where g, h are nonunit polynomials over $\mathbb{Z}$. Let $g(x) = \sum_{i=0}^{r} b_i x^i$ and $h(x) = \sum_{i=0}^{r} c_i x^i$. Since p divides $a_0 = b_0 c_0$ but not a_0^2, either p divides exactly one of b_0 and c_0 (w.l.o.g., we assume it divides b_0). Since p does not divide $a_n = b_r c_s$. Therefore, there exists an minimal $0 < t \leq r < n$ such that p does not divide b_t. By the Cauchy product, we can $a_t = b_t c_0 + \sum_{i=1}^{t} b_{t-i} c_i$. Since t was minimal, it divides $\sum_{i=1}^{t} b_{t-i} c_i$. Since p divides a_t, it must divide one of b_t and c_0, a contradiction. □

Theorem 118. *Let D be an integral domain and x, y be elements of D. Then,*

1. *x divides y if and only if $\langle y \rangle \subset \langle x \rangle$;*
2. *x is a unit if and only if $\langle x \rangle = D$.*

Proof. Suppose x divides y. That is, there exists t in D such that $y = tx$. Therefore, $y \in \langle x \rangle$ and hence $\langle y \rangle \subset \langle x \rangle$. Conversely, suppose $\langle y \rangle \subset \langle x \rangle$. □

Theorem 119. *Let F be a field and p be a polynomial over F. Then, $\langle p \rangle$ is a maximal ideal in $F[x]$ if and only if p is irreducible over F.*

Proof. Suppose p is irreducible and $\langle p \rangle$ is not maximal. Then, there exists an ideal B such that $\langle p \rangle \subsetneq B \subsetneq F[x]$. By Theorem 109, $F[x]$ is a PID and hence $B = \langle g \rangle$ for some polynomial

g over F. Since $\langle g \rangle \subsetneq F[x]$, by Theorem 118, g is not a unit. Also due to Theorem 118, since $\langle p \rangle \subset \langle g \rangle$, $p = fg$ for some polynomial f over F. However, p is irreducible, so that f must be a unit in $F[x]$. Therefore, $g = f^{-1}p$, and hence p divides g. By Theorem 118, $\langle g \rangle \subset \langle p \rangle$, a contradiction.

As for the converse, suppose $\langle p \rangle$ is a maximal ideal and $p = fg$ a factorization of p. Suppose that f and g are not units. Since $\langle p \rangle \subsetneq \langle f \rangle$ and $\langle p \rangle$ is maximal, $\langle f \rangle = F[x]$ by Theorem 118, and hence f is a unit, a contradiction. □

The above can be generalized for arbitrary PIDs in lieu of $F[x]$.

Theorem 120. *Let R be a commutative ring with unity and I an ideal. J is a maximal ideal if and only if R/J is a field.*

Corollary 121. *Let F be a field and p a polynomial over F. $F[x]/\langle p \rangle$ is a field.*

Proof. By Theorem 119 and Theorem 120. □

Definition 122 (Associates)**.** Two elements of an integral domain are said to be associates if they divide one another.

We can extend our definition of irreducibility as follows:

Definition 123 (Irreducible element)**.** A nonunit, nonzero element of an integral domain is said to be irreducible if it cannot be factored into a product of two nonunit elements. Otherwise, it is said to be reducible.

Definition 124 (Prime)**.** A nonunit element p of an integral domain is said to be prime if for all a and b also in the integral domain, if p divides a or b whenever it divides ab.

Note that in a general integral domain, primes and irreducibles need not coincide. However...

Theorem 125. *A prime in an integral domain is irreducible.*

Proof. Suppose p is prime and reducible, so that $p = ab$ for nonunit a and b. Therefore, p divides a or b. W.l.o.g., suppose p divides a so that $a = pt$ for some t. Equivalently, $a = abt$, or $a(1 - bt) = 0$. Since a is nonzero, $bt = 1$, and hence b is a unit. □

The converse also holds in a PID:

Theorem 126. *In a PID, an element is prime if and only if it is irreducible.*

Proof. Suppose a is an irreducible element of the PID, D. Suppose that a divides bc. Let $I = \{ax + by : x, y \in D\}$. Note that I is an ideal since if z is in I and r is an element of D, $zr = (ax + by)r = axr + byr$ is in I. Since D is a PID, $I = \langle p \rangle$ for some p. Since a is in I, $a = pr$ for some r. Since a is irreducible, d or r is a unit. If d is a unit, $I = D$. Therefore, $1 = ax + by$ so that $c = cax + cby$ so that a divides c. If r is a unit, $\langle a \rangle = \langle d \rangle = I$. Since b is in I, $at = b$ for some t and a divides b. □

Corollary 127. *Let F be a field and let a, b, and p be polynomials over F. If p is irreducible over F and p divides ab, then p divides a or b.*

Proof. $F[x]$ is a PID by Theorem 109. □

Definition 128 (Unique factorization domain)**.** A unique factorization domain (UFD) R is an integral domain in which every nonzero x in can be written

$$x = up_1 \cdots p_n \text{ where } u \text{ is a unit and } p_i \text{ is irreducible.}$$

This representation is unique in the sense that if $x = wq_1 \cdots q_n$ for w a unit and q_i irreducible, there exists a bijection $\varphi : \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that p_i and $q_{\varphi(i)}$ are associates.

Lemma 129 (Ascending chain condition)**.** *In a PID, any ascending chain of ideals $I_1 \subset I_2 \subset \cdots$ terminates (i.e. $I_n = I_{n+1}$ for some n).*

Proof. Note that $I = \bigcup_{i=1}^{\infty} I_i$ is an ideal, and therefore $I = \langle a \rangle$ for some element a in the PID. Since a is in I, a is in I_n for some n. Therefore, $\langle a \rangle \subset I_n$, and therefore $I_n = I$. □

We give the following without proof:

Theorem 130. *All PIDs are UFDs.*

Corollary 131. *Let F be a field. $F[x]$ is a UFD.*

Proof. By Theorem 109 and the above. □

The following structure generalizes Euclidean division:

Definition 132 (Euclidean domain)**.** An integral domain D is called a Euclidean domain if there is a function d from the nonzero elements of D to the nonnegative integers such that

1. $d(a) \leq d(ab)$ for all nonzero a, b in D;
2. if a, b are in D with $b \neq 0$, there exist q and r in D such that $a = bq + r$ with $r = 0$ or $d(r) < d(b)$.

Theorem 133. *A Euclidean domain is a PID.*

Proof. Let I be an ideal of a Euclidean domain D with $I \neq \{0\}$. Let b be an element of I with $b \neq 0$ and $d(b)$ minimal. Let a be in I. Write $a = bq + r$ where $r = 0$ or $d(r) < d(b)$. Then, $r = a - bq$ and hence r is in I. If $r \neq 0$, $d(r) < d(b)$, which contradicts the assumption that $d(b)$ is minimal in I. Therefore, $a = bq$. Since a was arbitrary, $I = \langle b \rangle$. □

We give the following without proof:

Theorem 134. *If D is a UFD, so too is $D[x]$.*