Algebra

Prof Atul Dixit[1]

Organized Results

complied by

Sarthak[2]

October 2022

To my stars,
Giuseppe, and the Doctor...

[1]adixit@iitgn.ac.in
[2]vijaysarthak@iitgn.ac.in

Contents

Chapter I

Groups

1 Powers in a group

August 11, 2022

Remark. *Unless stated otherwise, the group operation will be denoted by juxtaposition.*

Definition 1.1 (Semi-group)**.** A set with an associative binary operation.

Proposition 1.2. *A semi-group has at most one identity element. If it exists, then each element has at most one inverse.*

Definition 1.3 (Group)**.** A semi-group which has an identity and each of whose elements has an inverse.

Remark. *This allows to define, in a given group, the inverse of an element a as a^{-1}.*

Proposition 1.4. *Invertible elements od a semi-group form a group.*

Definition 1.5 (Powers)**.** Let G be a group and $a \in G$. Then for $n \in \mathbb{Z}$, we define

$$a^n := \begin{cases} e, & n = 0 \\ a^{n-1}, & n > 0 \\ (a^{-n})^{-1}, & n < 0 \end{cases}.$$

Remark. *The above "overloading" of a^{-1} is actually an extension. Hence we can interpret a^{-1} in either way.*

Proposition 1.6 (Properties of powers)**.** *Let G be a group and $a \in G$. Let $m, n \in \mathbb{Z}$. Then the following hold:*

(i) $(a^{-1})^{-1} = a$,

(ii) $a^{n\pm 1} = a^n a^{\pm 1}$,

(iii) $a^m a^n = a^{m+n}$,

(iv) $(a^n)^{-1} = a^{-n}$, *and*

(v) $(a^m)^n = a^{mn}$.

2 gcd, lcm, order...

August 15, 2022

Prove ***all*** *these!*

Definition 2.1 (gcd and lcm)**.** Let $a_1, \ldots, a_k \in \mathbb{Z}$ with $k \geq 1$. Then

(i) for a_i's not all zero, we define

$$\gcd(a_1, \ldots, a_k) := \max\{\text{common divisors of } a_i\text{'s}\}, \text{ and}$$

(ii) for each $a_i \neq 0$, we define

$$\operatorname{lcm}(a_1, \ldots, a_k) := \min\{\text{positive common multiples of } a_i\text{'s}\}$$

Proposition 2.2 (Properties of gcd)**.** *Let $a_1, \ldots, a_k \in \mathbb{Z}$ for $k \geq 1$, not all zero. Then the following hold:*

(i) We have

$$\gcd(a_1, \ldots, a_k) = \gcd(|a_1|, \ldots, |a_k|).$$

(ii) For $k \geq 2$, we have

$$\gcd(a_1, \ldots, a_k) = \gcd(\gcd(a_1, \ldots, a_{k-1}), a_k).$$

(iii) $\gcd(a_1, \ldots, a_k)$ *is the unique integer $d > 0$ such that*

- *(a) d is a common divisor of a_i's, and*
- *(b) each common divisor of a_i's divides d.*

Proposition 2.3 (Bézout's lemma)**.** *For $a, b \in \mathbb{Z}$ not both zero, there exist $m, n \in \mathbb{Z}$ such that*

$$\gcd(a, b) = ma + nb.$$

Proposition 2.4 (Properties of lcm)**.** *Let $a_1, \ldots, a_k \in \mathbb{Z} \setminus \{0\}$ for $k \geq 1$. Then*

(i) We have

$$\operatorname{lcm}(a_1, \ldots, a_k) = \operatorname{lcm}(|a_1|, \ldots, |a_k|).$$

(ii) For $k \geq 2$, we have

$$\operatorname{lcm}(a_1, \ldots, a_k) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{k-1}), a_k).$$

(iii) $\operatorname{lcm}(a_1, \ldots, a_k)$ *is the unique integer $m > 0$ such that*

(a) m is a common multiple of a_i's, and

(b) m divides each common multiple of a_i's.

Proposition 2.5. *Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then*

$$\gcd(a, b) \operatorname{lcm}(a, b) = |ab|.$$

Remark. *We'll take for granted the definition of $\mathbb{Z}_n$, and the multiplication operation on it. We'll also use Bézout's lemma. Also, we'll take the semantic definitions of the* lcm *and* gcd*.*

Proposition 2.6 (Multiplicative inverses in $\mathbb{Z}_n$)**.** *For $a, n \in \mathbb{Z}$ not both zero, we have that $\bar{a}$ is invertible $\iff$ $\gcd(a, b) = 1$.*

Theorem 2.7. $\mathbb{N}$ *is well-ordered.*

Definition 2.8 (Order of a group element)**.** Let G be a group and $a \in G$. Let

$$S := \{n > 0 : a^n = e\}.$$

Then we define

$$|a| := \begin{cases} \min S, & S \neq \emptyset \\ \infty, & S = \emptyset. \end{cases}$$

Theorem 2.9. *Let G be a group and $a \in G$ with $|a| < \infty$. Then for any $n \in \mathbb{Z}$, the following hold:*

(i) We have

$$a^n = e \iff |a| \mid n.$$

(ii) *We have*

$$|a^n| = \frac{|a|}{\gcd(|a|, n)}.$$

Result 2.10. The order of the product of commuting elements of a group divides the lcm of their respective orders.

If the orders are pairwise coprime, then the order is the product of the respective orders.

Result 2.11. Let G be a group and $a, b \in G$. Let $m \in \mathbb{Z}$ such that $aba^{-1} = b^m$. Then for any $n \geq 0$, we have

$$a^n b a^{-n} = b^{m^n}.$$

It follows that if $|a| \bigm| \alpha$, then $|b| \bigm| m^\alpha - 1$ for $\alpha \geq 0$.

3 Modular arithmetic

August 13, 2022

Definition 3.1 (Modulo congruence)**.** Let $a, b, n \in \mathbb{Z}$. Then we write

$$a \equiv b \mod n \quad \text{iff} \quad n \mid (a - b).$$

Proposition 3.2. *For any $n \in \mathbb{Z}$, congruence* $\bmod n$ *is an equivalence relation on* $\mathbb{Z}$*.*

Lemma 3.3. *Let $a, b, c \in \mathbb{Z}$ such that both of a, b are not zero with* $\gcd(a, b) = 1$*. Let $a \mid bc$. Then $a \mid c$.*

Proposition 3.4 (Properties of modulo congruence)**.** *Let $n, a, b, c \in \mathbb{Z}$. Then the following hold with all the congruences being taken with n:*

(i) $a \equiv b \iff a + c \equiv b + c$.

(ii) $a \equiv b \implies ac \equiv bc$.

(iii) $ac \equiv bc$ *and* $\gcd(n, c) = 1$ *with n, c not both zero* $\implies a \equiv b$.

Definition 3.5 (Modulo)**.** Let $n \in \mathbb{Z} \setminus \{0\}$ and $a \in \mathbb{Z}$. Then we define $a \bmod n$ to be the remainder obtained upon dividing a by n.

Proposition 3.6 (Properties of modulo)**.** *Let* $n \in \setminus\{0\}$ *and* $a, b \in \mathbb{Z}$*. Then the following hold:*

(i) $a \bmod n = b \bmod n \iff a \equiv b \mod n$.

(ii) $(a \bmod n) \bmod n = a \bmod n$.

(iii) $(a + b \bmod n) \bmod n = (a + b) \bmod n$.

(iv) $(a(b \bmod n)) \bmod n = ab \bmod n$.

Definition 3.7 (Prime integers)**.** $p \in \mathbb{Z}$ will be called prime iff $|p| \neq 1$ and the only divisors of p are ± 1, $\pm p$.

Proposition 3.8 ($\mathbb{Z}_n$ and U_n)**.** *Let* $n \in \mathbb{Z}$ *with* $|n| \neq 0$*. Then*

$$\mathbb{Z}_n := \{0, \dots, |n| - 1\}$$

forms an abelian group under the operation

$$(a, b) \mapsto (a + b) \bmod n,$$

and an abelian semi-group under the operation

$$(a, b) \mapsto (ab) \bmod n$$

with identity being 1 *if* $|n| > 1$ *and* 0 *if* $|n| = 1$*.*

Further, for $n \geq 1$*, the set*

$$U_n := \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$$

is the set of all invertible elements of $\mathbb{Z}_n$*, and for a prime* p*, we have that*

$$|U_p| = |p| - 1.$$

Remark. *Note that* $a \bmod 0$ *makes no sense, hence we couldn't define* $\mathbb{Z}_0$*. See however Definition 9.13 and Theorem 9.14.*

4 Permutation groups

August 12, 2022

Proposition 4.1. *The set of all permutations of a set forms a group under function composition.*

Notation. *For a set X, we'll denote by S_X the set of all permutations of X. For $n \in \mathbb{N}$, we'll use $S_n := S_{\{1,\dots,n\}}$.*

Definition 4.2 (Dynamic set)**.** Let σ be a permutation of a set A. Then we define the dynamic set of σ to be the set

$$\{a \in A : \sigma(a) \neq a\}.$$

Proposition 4.3. *Let σ be a permutation of a set A and K be the associated dynamic set. Then*

$$\sigma(K) = K.$$

Definition 4.4 (Disjoint permutations)**.** Two permutations on a set are called disjoint iff their associated dynamic sets are disjoint.

Theorem 4.5. *Disjoint permutations commute.*

Theorem 4.6 (Cycles in a permutation)**.** *Let σ be a permutation of a set A and K be the associated dynamic set. Define a relation $\sim_A$ (respectively $\sim_K$) on A (respectively K) by*

$$a \sim_A b \text{ (respectively } a \sim_K b\text{) iff } a = \sigma^n(b) \text{ for some } n \in \mathbb{Z}.$$

Then the following hold:

(i) The above are equivalence relations.

(ii) We have

$$\{\text{equivalence classes of } \sim_K\} \\ = \{\text{non-singleton equivalence classes of } \sim_A\}$$

(iii) If C is an equivalence class of $\sim_A$, then we have that

$$\sigma(C) = C$$

and hence we can restrict σ on C, obtaining a permutation on C, the dynamic set, L, of whose trivial extension is given by

$$L = \begin{cases} C, & C \text{ is non-singleton} \\ \emptyset, & \text{otherwise} \end{cases}.$$

(iv) The (trivial extensions of) restricted σ's above are disjoint permutations; such an extension is non-identity $\iff$ corresponding equivalence class is of $\sim_K$.

(v) *The composition, whenever finite, (in any order) of (the trivial extensions of) all the restricted σ's above (in K or in A) gives σ back.*

(vi) *Let C be an equivalence class of $\sim_A$. Let $a \in C$ and $n \geq 1$. Then the following are equivalent:*

   (a) *C has n elements.*

   (b) *$C = \{\sigma^0(a), \ldots, \sigma^{n-1}(a)\}$ with $\sigma^i(a)$'s being distinct.*

   (c) *n is the smallest positive integer k such that $\sigma^k(a) = a$.*

Remark. We call the equivalence classes of A, the cycles of σ. (Note that since σ is specified, mentioning only the set is sufficient.)

Theorem 4.7 (k-cycles)**.** *Let A be a set and $a_0, \ldots, a_{k-1} \in A$ be distinct for $k \geq 1$. Then there exists a unique function $\sigma\colon A \to A$ such that*

$$\sigma(x) = \begin{cases} a_{(i+1) \bmod k}, & x = a_i \text{ for some } 0 \leq i < k \\ x, & \text{otherwise} \end{cases}.$$

Further, the following hold:

(i) *σ is a permutation on A, with*

$$\sigma^{-1}(x) = \begin{cases} a_{(i-1) \bmod k}, & x = a_i \text{ for some } 0 \leq i < k \\ x, & \text{otherwise} \end{cases}.$$

(ii) *For any $i, j \in \mathbb{Z}$, we have*

$$\sigma^i(a_j) = a_{(i+j) \bmod k}.$$

(iii) *The cycle of σ containing a_0 is $\{a_0, \ldots, a_{k-1}\}$.*

(iv) *The trivial extension of the restriction of σ on $\{a_0, \ldots, a_{k-1}\}$ is σ itself.*

(v) *The order of σ is k.*

(vi) *The induced partition of the dynamic set is $\big\{\{a_0, \ldots, a_{k-1}\}\big\}$ if $k > 1$, and $\emptyset$ if $k = 1$.*

Notation. For a given A, this allows to denote σ by $(a_1, \ldots, a_k)$.

Remark. Note that 1-cycles are id.

Result 4.8. S_n is abelian $\iff n < 3$.

Proposition 4.9 (Finite cycles induce k-cycles)**.** *Let σ be a permutation of a set A and C be a cycle with k elements. Then the trivial extension of the restriction of σ on C is a k-cycle.*

Theorem 4.10. *Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Then there exists a unique finite set of disjoint non-identity k-cycles (for possibly different k's) in $\{1, \ldots, n\}$ whose product is σ.*

Definition 4.11 (Transpositions)**.** 2-cycles in a set are called transpositions.

Theorem 4.12 (Decomposing finite cycles in transpositions)**.** *Let A be a set and $a_0, \ldots, a_{k-1} \in A$ be distinct for $k \geq 1$. Then*

$$(a_0, \ldots, a_{k-1}) = (a_0, a_{k-1}) \ldots (a_0, a_1).$$

Corollary 4.13. *Any permutation in S_n can be decomposed as a finite product of transpositions.*

Definition 4.14 (Odd and even permutations)**.** Let $n \in \mathbb{N}$. Then a $\sigma \in S_n$ is called odd (respectively even) iff it can be written as a finite product of an odd (respectively even) number of transpositions.

Proposition 4.15 (Permutation matrices and S_n)**.** *Let $n \geq 1$. Define a function $P \colon S_n \to M_{n\times n}(\mathbb{Z})$ by*

$$(P_\sigma)_i := (e_{\sigma(i)})^t.$$

Then P is injective and we have

$$P_\sigma P_\tau = P_{\tau\sigma}.$$

Theorem 4.16. *$\sigma \in S_n$ for $n \geq 0$ can't be both, odd and even.*

Proposition 4.17 (Alternating groups)**.** *Let $n \in \mathbb{N}$. Then*

$$A_n := \{\sigma \in S_n : \sigma \text{ is even}\}$$

forms a group with

$$|A_n| = \frac{n!}{2}.$$

5 Subgroups

Definition 5.1 (Subgroups)**.** Let G be a group. Then a subset $H \subseteq G$ is called a subgroup of G, written $H \leq G$ iff the following hold:

(i) G's operation can be inherited to H, and

(ii) H forms a group under the inherited operation.

Proposition 5.2. *The identities and inverses in a subgroup are the same as those in the parent group.*

Remark. *This allows to use the same notation for the group operation, the identity and the inverses as those in the parent group.*

Proposition 5.3 (Characterizing subgroups)**.** *Let G be a group and $H \subseteq G$ be nonempty. Then the following are equivalent:*

(i) $H \leq G$*.*

(ii) $ab^{-1} \in H$ *for any* $a, b \in H$*.*

(iii) H *is closed under* G*'s operation and taking inverses.*

Result 5.4. If G is a finite group, then ab^{-1} above can be replaced with ab.

Proposition 5.5.

(i) Subgroup of a subgroup is a subgroup.

(ii) Nonempty intersection of subgroups is a subgroup.

Result 5.6 (Unions almost never form subgroups)**.** Let G be a group and $H, K \leq G$. Then

$$H \cup K \leq G \iff H \subseteq K \text{ or } K \subseteq H.$$

Theorem 5.7 (Subgroups generated by sets)**.** *Let G be a group and $S \subseteq G$. Then*

$$\langle S \rangle := \bigcap \{H \leq G : H \supseteq S\}$$

is the smallest subgroup of G that contains S.

Further, we have that

$$\langle S \rangle = \{\text{“finite strings” of elements in } S \text{ and their inverses}\}.$$

Proposition 5.8. *Let G be a group. Then*

(i) $H, K \leq G$ *and* $H \subseteq K \implies H \leq K$,

(ii) $H \subseteq K \subseteq G \implies \langle H \rangle \leq \langle K \rangle$, *and*

(iii) $H \leq G \implies \langle H \rangle = H$.

Result 5.9. For $n \geq 3$, the group A_n is generated by 3-cycles.

Remark. *For $a_1, \ldots, a_n \in G$, we'll often denote $\langle \{a_1, \ldots, a_n\} \rangle$ by $\langle a_1, \ldots, a_n \rangle$.*

Proposition 5.10 (The subgroup $\langle a \rangle$)**.** *Let G be a group and $a \in G$. Then*

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Theorem 5.11. *Let G be a group and $a \in G$. Then the following hold:*

(i) $|a| < \infty \implies \langle a \rangle = \{a^0, \ldots, a^{|a|-1}\}$.

(ii) $|a| < \infty \iff |\langle a \rangle| < \infty$.

(iii) $|a|, |\langle a \rangle| < \infty \implies |a| = |\langle a \rangle|$,

Proposition 5.12. *An infinite group has infinitely many subgroups.*

Notation. *We'll use the usual notation $n\mathbb{Z}$.*

Theorem 5.13. *The subgroups of $\mathbb{Z}$ are precisely $n\mathbb{Z}$ for $n \in \mathbb{Z}$.*

6 Product of subgroups

Definition 6.1 (Product of subsets)**.** Let G be a group and $A, B \subseteq G$. Then we define

$$AB := \{ab : a \in A, b \in B\}, \text{ and}$$
$$A^{-1} := \{a^{-1} : a \in A\}.$$

Remark. *Even if $H, K \leq G$ for a group G, we don't need to have $HK \leq G$: Take any $\{e, a\}, \{e, b\} \leq G$ with $ab \neq ba$.*

Proposition 6.2 (Properties of products of subsets)**.** *Let G be a group and $A, B, C \subseteq G$. Then the following hold:*

(i) $A \subseteq B \implies AC \subseteq BC$ *and* $CA \subseteq CB$.

(ii) $(AB)C = A(BC)$, *and*

(iii) $(AB)^{-1} = B^{-1}A^{-1}$.

Proposition 6.3 (Another characterization of subgroups)**.** *Let H be a nonempty subset of a group G. Then the following are equivalent:*

(i) $H \leq G$.

(ii) $HH^{-1} \subseteq H$.

(iii) $HH = H$ *and* $H^{-1} = H$.

Theorem 6.4 (When is HK a subgroup?)**.** *Let $H, K \leq G$ for a group G. Then the following are equivalent:*

(i) $HK \leq G$.

(ii) $HK = KH$.

(iii) $KH \leq G$.

Proposition 6.5 (Center of a group)**.** *Let G be a group and*

$$Z_G := \{g \in G : gh = hg \text{ for all } h \in G\}.$$

Then

$$Z_G \leq G.$$

7 Cyclic groups

Definition 7.1 (Cyclic group)**.** A group G is called cyclic iff there exists a $a \in G$ such that

$$G = \langle a \rangle.$$

Proposition 7.2. *Cyclic groups are abelian.*

Remark. *Converse needn't be true: Consider V, the Klein four-group.*

Theorem 7.3. *Let G be a finite group and $a \in G$. Then*

$$G = \langle a \rangle \iff |G| = |a|.$$

Proposition 7.4. *Let G be a group and $a \in G$ with $|a| < \infty$. Then for any $k \in \mathbb{Z}$, we have*

$$G = \langle a^k \rangle \iff \gcd(|a|, k) = 1.$$

Theorem 7.5 (Subgroups of cyclic groups are cyclic)**.** *Let G be a cyclic group and $a \in G$ such that $G = \langle a \rangle$. Let $H \leq G$ with $H \neq \{e\}$. Then*

$$S := \{n \geq 1 : a^n \in H\}$$

is nonempty, and

$$H = \langle a^{\min S} \rangle.$$

Theorem 7.6. *A group having no non-trivial subgroups is finite cyclic and has prime order.*

Proposition 7.7 ("Converse" of Lagrange for cyclic)**.** *Let G be a finite cyclic group and $m \geq 1$ such that $m \mid |G|$. Then there exists a unique subgroup H of G such that $|H| = m$.*

8 Cosets

August, 19, 2022

Definition 8.1 (Cosets)**.** Let G be a group, $A \subseteq G$ and $g \in G$. Then we define

$$gA := \{g\}A, \text{ and}$$
$$Ag := A\{g\}.$$

Proposition 8.2 (Properties of cosets)**.** *Let G be a group, $H \leq G$ and $a \in G$. Then the following hold:*

(i) The following are equivalent:
   - *(a) $aH = H$.*
   - *(b) $a \in H$.*
   - *(c) $Ha = H$.*

(ii) The following are equivalent:
   - *(a) $aH = bH$.*
   - *(b) $a^{-1}b \in H$.*
   - *(c) $aH \cap bH \neq \emptyset$.*

(iii) The following are equivalent:

(a) $Ha = Hb$.
(b) $ab^{-1} \in H$.
(c) $Ha \cap Hb \neq \emptyset$.

Proposition 8.3 (Partitioning via cosets)**.** *Let G be a group and $H \leq G$. Let*

$$\Pi_L := \{aH : a \in G\}, \text{ and}$$
$$\Pi_R := \{Ha : a \in G\}.$$

Then the following hold:

(i) Π_L *and* Π_R *are partitions of* G.
(ii) $|\Pi_L| = |\Pi_R|$.
(iii) $|aH| = |H| = |Ha|$.

Definition 8.4 (Index of a subgroup)**.** Let G be a group and $H \leq G$. Then we define

$$[G : H] := \big|\{\text{left (or right) cosets of } H\}\big|.$$

Theorem 8.5 (Lagrange's theorem)**.** *Let G be a group and $H \leq G$. Then the following hold:*

(i) $|G| < \infty \iff |H|, [G : H] < \infty$.
(ii) *If* $|G|, |H|, [G : H] < \infty$, *then*

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

Proposition 8.6 (Immediate consequences)**.**

(i) *If G is a finite group and $a \in G$, then* $|a| \mid |G|$.
(ii) *Groups of prime order are cyclic.*
(iii) *(Fermat's little theorem) If p is a prime and $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

(iv) *Let G be a group and $H, K \leq G$ with* $\gcd(|H|, |K|) = 1$. *Then we have that*

$$H \cap K = \{e\}.$$

Result 8.7. A group with a prime power order, say p^n with $n \geq 1$, has an element of order p.

Proposition 8.8. *Let G be a group and $H, K \leq G$. Then the following hold:*

(i) $H \cap K \leq H, K$.

(ii) $|HK| < \infty \iff |H|, |K| < \infty$.

(iii) If $|H|, |K|, |HK|, |H \cap K| < \infty$, *then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Result 8.9 ("Converse" of Lagrange's theorem need not hold)**.** A_4, that has 12 elements, doesn't have any subgroup of order 6.

9 Normal subgroups

August 29, 2022

Definition 9.1. Normal subgroups A subgroup H of a group G is called normal, written $H \trianglelefteq G$, iff $gH = Hg$ for all $g \in G$.

Corollary 9.2 (Immediate results)**.**

(i) Subgroups of abelian groups are normal.

(ii) Center of a group is a normal subgroup.

Result 9.3 (A normal subgroup of a non-abelian group)**.** We have

$$\{\mathrm{id}, (123), (132)\} \trianglelefteq S_3.$$

Result 9.4. Let G be a group and $H \leq G$ such that $[G : H] = 2$. Then $H \trianglelefteq G$.

Remark. *Subgroup of a normal subgroup needn't be normal: Otherwise, each subgroup would be normal.*

Normal subgroup of a normal subgroup needn't be normal.[1]

Theorem 9.5 (Characterizing normal subgroups)**.** *Let G be a group and $H \leq G$. Then the following are equivalent:*

[1] D_4 provides a minimal example. See here.

(i) $H \trianglelefteq G$.
(ii) $gHg^{-1} \subseteq H$ *for all* $g \in G$.
(iii) $gHg^{-1} = H$ *for all* $g \in G$.
(iv) *Every left (respectively right) coset is a right (respectively left) coset.*

Proposition 9.6. *Nonempty intersections of normal subgroups are normal.*

Theorem 9.7. *Let* G *be a group and* $H, K \leq K$. *Then the following hold:*
(i) $H \trianglelefteq G \implies HK \leq G$.
(ii) $H, K \trianglelefteq G \implies HK \trianglelefteq G$.

Result 9.8. Let G be a group and $H \trianglelefteq G$ with $[G : H]$ being prime. Then for any $K \leq G$, we have either $K \leq H$, or $G = HK$.

Notation. *For* $H \trianglelefteq G$, *the left and the right cosets coincide and hence we can denote the partition by* G/H, *and equivalence classes* aH *by* $\bar{a}$.

Proposition 9.9 (Quotient groups)**.** *Let* G *be a group and* $H \trianglelefteq G$. *Then the binary operation on* G/H *given by*

$$(\bar{a}, \bar{b}) \mapsto \overline{ab}.$$

is well-defined and G/H *forms a group under this operation.*

Result 9.10. Let G be a group such that G/Z is cyclic. Then G is abelian.

Result 9.11. Let G be a group and $H \leq G$ such that $a^2 \in H$ for all $a \in G$. Then $H \trianglelefteq G$ and G/H is abelian.

Proposition 9.12 ($\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$)**.** *Let* $n \in \mathbb{Z} \setminus \{0\}$. *Then*

$$a \mapsto \bar{a}$$

is a bijection $\mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ *that preserves addition as well as multiplication, i.e.,*

$$(a + b) \bmod n \mapsto \bar{a} + \bar{b}, \text{ and}$$
$$ab \bmod n \mapsto \bar{a}\bar{b}.$$

Definition 9.13 (Defining $\mathbb{Z}_0$)**.** We define

$$\mathbb{Z}_0 := \mathbb{Z}.$$

Theorem 9.14. *For any* $n \in \mathbb{Z}$, *we have*

$$\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}.$$

Chapter II

Group homomorphisms

1 Basics

August 29, 2022

Definition 1.1 (Group homomorphisms)**.** Let $(G, *)$ and $(H, \circ)$ be groups. then a function $\phi\colon G \to H$ is called a group homomorphism iff the following diagram commutes.

$$\begin{tikzcd} G \times G \arrow[r, "\phi\times\phi"] \arrow[d, "*"'] & H \times H \arrow[d, "\circ"] \\ G \arrow[r, "\phi"'] & H \end{tikzcd}$$

That is,

$$\phi(a * b) = \phi(a) \circ \phi(b).$$

Corollary 1.2.

(i) *Compositions of group homomorphisms are group homomorphisms.*

(ii) *Restriction of a group homomorphism to subgroups of domain and codomain is a group homomorphism.*

(iii) *The identity map on a group is a group homomorphism.*

Proposition 1.3. *Let $\phi\colon G \to H$ be a group homomorphism. Let $a \in G$. Then the following hold:*

(i) $\phi(e) = e$.

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

(iii) $\phi(a^n) = \phi(a)^n$ *for* $n \in \mathbb{Z}$.

Theorem 1.4 (Preservations under homomorphisms)**.** *Under a group homomorphism,*

(i) subgroups are preserved both ways,

(ii) normal subgroups are preserved in the backward direction,

(iii) cyclicity and abelian-ness are preserved in forward direction, and

(iv) order of the image of, say g, divides the order of g.

Remark. *The inverse image of normal subgroups needn't be normal: Otherwise each subgroup of any group would be normal.*

Similarly for abelian, cyclic.

Proposition 1.5. *Under a surjective group homomorphism, the indices of subgroups are preserved.*

Definition 1.6. For a group homomorphism $\phi\colon G \to H$, we define

$$\ker\phi := \phi^{-1}(\{e\}).$$

Corollary 1.7. *Let $\phi\colon G \to H$ be a group homomorphism. Then*

$$\begin{aligned} \operatorname{im}\phi &\leq H, \text{ and} \\ \ker\phi &\trianglelefteq G. \end{aligned}$$

Proposition 1.8. *A group homomorphism is injective $\iff$ its kernel is $\{e\}$.*

Definition 1.9 (Group isomorphisms)**.** A group isomorphism is a bijective group homomorphism.

An isomorphism from a group to itself is called an *automorphism*.

A group G is said to be *isomorphic* to a group G iff there exists a group isomorphism $G \to H$.

Example 1.10. Conjugation is a group automorphism.

Proposition 1.11. *The inverse of a group isomorphism is a homomorphism.*

Proposition 1.12. *"Being isomorphic" is an equivalence relation for groups.*

Notation. *We'll denote this equivalence by "$\cong$".*

Proposition 1.13 (Preservations under isomorphisms)**.** *All the preservations in Theorem 1.4 hold in both directions.*

Result 1.14. Let G be a group and H be the unique subgroup of G having a given cardinality. Then $H \trianglelefteq G$.

Result 1.15. Any infinite cyclic group is isomorphic to $\mathbb{Z}$.

Result 1.16. Any group of order 4 is isomorphic to either $\mathbb{Z}_4$ or K_4.

Result 1.17. Any group of order 6 is isomorphic to either $\mathbb{Z}_6$ or to S_3.

Theorem 1.18 (Cayley)**.** *Any group G is isomorphic to some subgroup of S_G, a possible isomorphism being*

$$a \mapsto \phi_a \text{ defined by } \phi_a(g) := ag.$$

2 Isomorphisms theorems

September 9, 2022

Lemma 2.1 ("Quotienting" a domain with a function)**.** *Let $f\colon X \to Y$ be surjective, and define $\sim$ on X as*

$$x_1 \sim x_2 \iff f(x_1) = f(x_2).$$

Then $\sim$ is an equivalence relation and there exists a unique function $g\colon X/\sim \to Y$ such that

$$\begin{tikzcd} & X \arrow[dl, "\bar{x} \leftarrow x"'] \arrow[dr, "f"] & \\ X/\sim \arrow[rr, dashed, "g"'] & & Y \end{tikzcd}$$

commutes. This g is a bijection and

$$\bar{x} \overset{g}{\longmapsto} f(x).$$

Lemma 2.2. *Let $\phi\colon G \to H$ be a surjective group homomorphism. Then*

$$G/\ker\phi = G/\sim \text{, with}$$
$$g(\ker\phi) = [g]_\sim$$

where $\sim$ is as in Lemma 2.1.

Theorem 2.3 (First isomorphism theorem)**.** *Let $\phi\colon G \to H$ be a surjective group homomorphism. Then we have the following commutative diagram:*

$$\begin{tikzcd} & G \arrow[dl, "\bar{g} \leftarrow\!\shortmid g"'] \arrow[dr, "\phi"] & \\ G/\ker\phi \arrow[rr, dashed, "\sim", "\bar{g}\mapsto\phi(g)"'] & & H \end{tikzcd}$$

Result 2.4.

(i) For $n \geq 1$,
$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

(ii) Any finite cyclic group G is isomorphic to $\mathbb{Z}_{|G|}$.

Remark. *In writing conclusions of implication-based theorems, we'll omit explicitly mentioning "$H \trianglelefteq G$", and directly write statements about G/H.*

Theorem 2.5 (Second isomorphism theorem)**.** *Let G be a group, $H \leq G$ and $K \trianglelefteq G$. Then*
$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Theorem 2.6 (Third isomorphism theorem)**.** *Let $H, K \trianglelefteq G$ for a group G with $H \subseteq K$. Then*
$$\frac{G/H}{K/H} \cong \frac{G}{K}.$$

3 Direct products

3.1 External direct products

September 17, 2022

Proposition 3.1 (External direct product)**.** *Let G, H be groups. Then $G \times H$ forms a group under the operation*
$$\big((g_1, h_1), (g_2, h_2)\big) \mapsto (g_1g_2, h_1h_2).$$

Proposition 3.2. *For groups G, H, K, we have*

$$G \times H \cong H \times G, \text{ and}$$
$$(G \times H) \times K \cong G \times (H \times K).$$

Further, G and H sit as normal subgroups inside $G \times H$.

Proposition 3.3. *For groups, $G_1 \cong G_2$ and $H_1 \cong H_2 \implies G_1 \times H_1 \cong G_2 \times H_2$.*

Theorem 3.4 (Order of elements in $G \times H$)**.** *Let G, H be groups and $(g, h) \in G \times H$. Then in the group $G \times H$,*

$$|(g, h)| = \operatorname{lcm}(|g|, |h|).$$

Theorem 3.5. *Let $m, n \in \mathbb{Z}$. Then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic $\iff \gcd(m, n) = 1$.*

3.2 Internal direct products

Proposition 3.6 (Internal direct product)**.** *Let G be a group and $H, K \leq G$ such that $G = HK$ and $H \cap K = \{e\}$. Then the following are equivalent:*

(i) $H, K \trianglelefteq G$.

(ii) $hk = kh$ *for all* $h \in H$, $k \in K$.

Lemma 3.7. *Let $\phi \colon G \to G'$ be an injective homomorphism, and $H \trianglelefteq G$. Then*

$$G/H \cong \phi(G)/\phi(H).$$

Theorem 3.8. *Let G be an internal direct product of the subgroups H, K. Then the following hold:*

$$HK = G \cong H \times K$$
$$\frac{HK}{K} \cong H \cong \frac{H \times K}{\{e\} \times K}$$
$$\frac{HK}{H} \cong K \cong \frac{H \times K}{H \times \{e\}}$$

Proposition 3.9. *Any abelian group of order 8 is isomorphic to $\mathbb{Z}_8$, or to $\mathbb{Z}_2 \times \mathbb{Z}_4$, or to $\mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_2)$.*

Chapter III

Group actions

1 Basics

October 4, 2022

Definition 1.1 (Group actions, orbits, stabilizers)**.** Let G be a group and X a set. Then a function $G \times X \to X$

$$(g, x) \mapsto gx$$

is called a (left) action of G on X iff

(i) $ex = x$, and

(ii) $g(hx) = (gh)x$.

Similarly, there are right actions.

For an $x \in X$, we define

$$\operatorname{orb}(x) := \{gx : g \in G\}, \text{ and}$$
$$\operatorname{stab}(x) := \{g \in G : gx = x\}.$$

We call the action *transitive*, iff some orbit covers then entire G. We call the action *free* iff each stabilizer is trivial, *i.e.*, $\{e\}$.

Corollary 1.2. *For a group action,* $\operatorname{orb}(x) = x \iff \operatorname{stab}(x) = G$.

Proposition 1.3 (Restricting actions)**.** *Let G be a group acting on a set X. Let $H \leq G$ and $x \in X$. Then we can restrict the action in two ways: $H \times X \to X$, and $G \times \operatorname{orb}(x) \to \operatorname{orb}(x)$.*

Theorem 1.4 (Facts about actions)**.** *Let G be a group acting on a set X. Then the following hold:*

(i) Orbits are precisely the equivalence classes of the following equivalence relation on X:

$$x \sim y \text{ iff } x = gy \text{ for some } g \in G.$$

(ii) Stabilizers are subgroups of G.

(iii) $[G : \mathrm{stab}(x)] = |\mathrm{orb}(x)|$ for each $x \in X$.

Example 1.5 (Translations and conjugations)**.** Consider a group G. Then the following are actions by G on X:

$$\begin{aligned} (g,h) &\mapsto gh & X &= G \\ (g,hK) &\mapsto ghK & X &= \{hK : h \in G, K \leq G\} \\ (g,h) &\mapsto ghg^{-1} & X &= G \\ (g,H) &\mapsto gHg^{-1} & X &= \{H : H \leq G\} \end{aligned}$$

Example 1.6 (Double cosets)**.** Let G be a group and $H, K \leq G$. Then $H \times K$ acts on G via

$$((h,k),x) \mapsto hxk^{-1}$$

and the orbits here are the double cosets HxK's.

Result 1.7. Let G be a finite group and $H < G$. Then

$$\bigcup_{x \in G} xHx^{-1} \subsetneq G.$$

2 The class equation

October 5, 2022

Definition 2.1 (Conjugacy classes)**.** Let G be a group and $x \in G$. Then we define

$$\mathrm{cl}(x) := \{gxg^{-1} : g \in G\}.$$

Corollary 2.2. *Conjugacy classes are precisely the orbits under conjugation.*

Theorem 2.3 (Class equation)**.** *Let G be a group. Then*

$$\{Z\} \cup \{\mathrm{cl}(x) : x \in G \setminus Z\}$$

forms a partition of G.

Result 2.4 (Centers of p-groups are non-trivial)**.** Let G be a finite group with $|G|$ being some honest p-power where p is a prime. Then $p \bigm| |Z|$.

Result 2.5 (Classifying groups with p^2 elements)**.** Let G be a finite group with $|G| = p^2$ where p is a prime. Then $G \cong \mathbb{Z}_p$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Result 2.6. Let G be a finite group having 3 conjugacy classes. Then $|G| \leq 6$.

3 Partial converses to Lagrange's theorem

October 5, 2022

Theorem 3.1 (Cauchy)**.** *Let G be a finite group and p be a positive prime dividing $|G|$. Then there exists an $x \in G$ such that $|x| = p$.*

Result 3.2. Let G be a finite group with $|G| = pn$ where p is a positive prime and $n < p$. Then G has a unique (and hence normal) subgroup of order p.

Lemma 3.3 (How do subgroups of G/H look like?)**.** *Let G be a group and $H \trianglelefteq G$. Then any subgroup of G/H is of the form K/H for some $K \leq G$ such that $K \supseteq H$.*

Theorem 3.4. *For finite abelian groups, the converse of Lagrange's theorem (Theorem 1.4) holds.*

3.1 Sylow theorems

October 5, 2022

Lemma 3.5. *Let p be a prime and $n \geq 0$. Let $a, b \in \mathbb{Z}$ such that $p^n \mid ab$ but $p^n \nmid a$. Then $p \mid b$.*

Theorem 3.6 (Sylow's first)**.** *Let G be a finite group. Let p be a positive prime and $n \geq 0$ such that $p^n \bigm| |G|$. Then there exists an $H \leq G$ such that $|H| = p^n$.*

Definition 3.7 (p-groups)**.** For a positive prime p, a group is called a p-group iff each of its elements has a p-power order.

Definition 3.8 (Sylow p-subgroups)**.** Let G be a group and p be a positive prime. Then an $H \leq G$ is called a Sylow p-subgroup of G iff H is a maximal (with respect to inclusion) p-subgroup of G.

The set of all p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$.

Proposition 3.9. *Let G be a finite group and p be a positive prime. Then G is a p-group $\iff$ $|G|$ is some p-power.*

Proposition 3.10 (Normalizers and centralizers)**.** *Let G be a group. Let $x \in G$ and $H \leq G$. Then*

$$\begin{aligned} C(x) &:= \{g \in G : gx = xg\}, \text{ and} \\ N(H) &:= \{g \in G : gH = Hg\} \end{aligned}$$

are subgroups of G, being the stabilizers of G's conjugation action.

Further, $C(x)$ is the largest subgroup of G in which x is in the center, and $N(H)$ is the largest subgroup of G in which H is normal.

Proposition 3.11. *Let P be a Sylow p-subgroup of a group G, for a positive prime p, such that $|N(P)| < \infty$. Then $p \nmid |N(P)/P|$.*

Proposition 3.12. *Isomorphisms preserve p-group-ness as well as Sylow p-subgroup-ness.*

Lemma 3.13. *Let G be a finite group, and P, Q be Sylow p-subgroups of G for a positive prime p. Then Q acts on $\mathcal{P} := \{xPx^{-1} : x \in G\}$ via conjugation, and for any $T \in \mathcal{P}$, we have that*

$$\mathrm{orb}(T) = \{T\} \iff Q = T.$$

Theorem 3.14 (Sylow's second and third)**.** *Let G be a finite group and p be a positive prime. Let $P \in \mathrm{Syl}_p(G)$ and $\mathcal{P}$ be the set of conjugates of P. Then the following hold:*

(i) $|\mathcal{P}| \equiv 1 \pmod{p}$.

(ii) $\mathrm{Syl}_p(G) = \mathcal{P}$.

Corollary 3.15. *Let G be a finite group and p be a positive prime. Let p^n be the largest p-power that divides G. Then*

$$\mathrm{Syl}_p(G) = \{H \leq G : |H| = p^n\}.$$

Result 3.16 (Normalization is idempotent for Sylow subgroups)**.** Let G be a group and $P \in \mathrm{Syl}_p(G)$ for a positive prime p. Then

$$N(N(P)) = N(P).$$

Theorem 3.17 (Classifying groups with pq elements)**.** *Let G be a finite group with $|G| = pq$ where $p < q$ are positive primes. Then there exist $a, b \in G$ and $1 \leq r < q$ such that*

(i) $G = \langle a, b \rangle$,

(ii) $a^p = e = b^q$,

(iii) $a^{-1}ba = b^r$, *and*

(iv) $r^p \equiv 1 \pmod q$.

4 Simple groups

October 6, 2022

Definition 4.1 (Simple groups)**.** A group is called simple iff it has no non-trivial normal subgroups.

Proposition 4.2. *Simple abelian groups are precisely $\mathbb{Z}_p$ for prime p's.*

Lemma 4.3 (Self-inverse bijections partition the set)**.** *Let X be a set and $f \colon X \to X$ such that $f \circ f = \mathrm{id}$. Then the following hold:*

(i) $\mathcal{C} := \{\{x, f(x)\} : x \in X\}$ *is a partition of X.*

(ii) For each $A \in \mathcal{C}$, define $\overline{f|_A}$ to be the trivial extension of $f|_A$. These $\overline{f|_A}$'s commute with each other.

(iii) If $\mathcal{C}$ is finite, then

$$f = \prod_{A \in \mathcal{C}} \overline{f|_A}.$$

Theorem 4.4 ($|G| = 2(\text{odd}) \implies$ not simple)**.** *Let G be a finite group of even order with $|G|/2$ being odd. Then G has a normal subgroup of order n.*

Theorem 4.5 (Cayley's extended)**.** *Let G be a group and $H \leq G$. Then there exists a homomorphism $\tau \colon G \to S_{\{gH : g \in G\}}$ with $\ker \tau \subseteq H$.*

Result 4.6. Let G be a finite group and $H \leq G$ such that $[G : H] \neq 1$ and $|G| \nmid [G : H]!$. Then G is not simple.

Result 4.7. Let G be a finite group and p be a positive prime dividing $|G|$ such that $|G| \nmid |\mathrm{Syl}_p(G)|!$. Then G is not simple.

Theorem 4.8 (Ernst Strauss)**.** *Let G be a finite group and $H \leq G$ such that $[G : H]$ is the smallest (positive) prime dividing $|G|$. Then $H \trianglelefteq G$.*

5 $|G| = p^n q$ violates simplicity

October 6, 2022

Theorem 5.1. *Let G be a finite p-group for a positive prime p and $H < G$. Then*

$$N(H) \supsetneq H.$$

Theorem 5.2. *Let G be a finite group and p be a positive prime. Then*

$$\bigcap \mathrm{Syl}_p(G) \trianglelefteq G.$$

Theorem 5.3 (Miller)**.** *Let G be a finite group with $|G| = p^n q$ for positive primes p, q and $n \geq 1$. Then G is not simple.*

Chapter IV

Rings

1 Basics

October 12, 2022

Definition 1.1 (Rings)**.** Let R be a set along with binary operations of addition and multiplication. Then R is called a ring iff the following hold:

(i) $(R, +)$ is an abelian group.

(ii) $(R, \cdot)$ is a semi-group.

(iii) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

R is called *commutative* iff $\cdot$ is commutative.

R is said to have an identity iff $\cdot$ has an identity.

We call the additive (respectively multiplicative) identity as *zero* (respectively *one*).

Notation. *We'll denote often zero by* 0 *and one by* 1*. We'll denote additive inverse of* a *by* $-a$*, and multiplicative inverse (if existent), by* a^{-1}*, and call them respectively negation and inverse of* a*.*

We'll also omit parentheses in $(a \cdot b) + (c \cdot d)$*, etc. assuming the usual convention that multiplication precedes over addition.*

We'll also drop the $\cdot$ *as usual and just denote that by juxtaposition.*

Remark. *It's unfortunate that the same juxtaposition is used for both* na*, and* ab*. To alleviate some of the confusion, we'll sometimes use* 0_R *and* 1_R*, and* $n_{\mathbb{Z}}$ *while (left) multiplying ring elements by these.*

Example 1.2 (One-sided inverses[1]). Consider the vector space $\mathbb{R}^{\mathbb{N}}$ over $\mathbb{R}$. Then the linear operators f, g in the ring[2] $\mathcal{L}(\mathbb{R}^{\mathbb{N}}, \mathbb{R}^{\mathbb{N}})$ defined by

$$f\colon (x_0, x_1, x_2 \dots) \mapsto (x_1, x_2, x_3, \dots), \text{ and}$$
$$g\colon (x_0, x_1, x_2 \dots) \mapsto (0, x_0, x_1, \dots)$$

are only invertible from one side.

Proposition 1.3. *Let R be a ring. Then*

(i) $0_R x = 0_R = x 0_R$.

(ii) $(-1_R)x = -x = x(-1_R)$ *(if R has identity 1_R).*

(iii) $(-a)b = -(ab) = a(-b)$.

(iv) $(-a)(-b) = ab$.

Remark. *Note that the ring multiplication by 0_R and $\pm 1_R$ yield exactly the same result that we get by integer multiplication by 0 and ± 1.*

Proposition 1.4 (Generalized distributivity). *Let R be a ring and $a_1, \dots, a_m, b_1, \dots, b_n \in R$ for $m, n \geq 0$. Then we have*

$$\Big(\sum_{i=1}^{m} a_i\Big)\Big(\sum_{j=1}^{n} b_j\Big) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j.$$

Proposition 1.5 (Rings form associative $\mathbb{Z}$-algebras). *Let R be a ring and $a, b \in R$. Then for any $m, n \in \mathbb{Z}$, we have*

$$(ma)(nb) = (mn)(ab).$$

Remark. *Note that na is defined for each $n \in \mathbb{Z}$. However, a^n may only be defined for $n \geq 1$.*

[1] Also see Example 3.2

[2] This is in fact an $\mathbb{R}$-algebra!

Result 1.6 (Binomial theorem for commutative rings)**.** Let R be a commutative ring and $a, b \in R$. Then for any $n \geq 1$, we have

$$(a+b)^n = a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i b^{n-i} + b^n.$$

If R further has identity, then for any $n \geq 0$, we have

$$(a+b) = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Proposition 1.7 (Characterizing the zero ring)**.** *Let R be a ring. Then*

$$R = \{0_R\} \iff R \text{ has identity and } 1_R = 0_R.$$

Definition 1.8 (Ring characteristic)**.** Let R be a ring. Let $S := \{n \geq 1 : na = 0_R \text{ for all } a \in R\}$. Then we define

$$\operatorname{char} R := \begin{cases} 0, & S = \emptyset \\ \min S, & S \neq \emptyset \end{cases}.$$

Proposition 1.9. *Let R be a ring. Then the following hold:*

(i) $\operatorname{char} R = 0 \implies |R| = \infty$.

(ii) $\operatorname{char} R \neq 0$ *and R has identity 1_R* $\implies$ $\operatorname{char} R$ *is precisely the order of 1_R in the additive group $(R, +)$.*

Result 1.10. Let R be a commutative ring with prime characteristic p. Then we have

$$(a+b)^p = a^p + b^p.$$

Example 1.11 (The rings $\mathbb{Z}_n$)**.** Let $n \in \mathbb{Z}$. Then $\mathbb{Z}_n$ forms a ring under the n-modulo addition and multiplication. Here, the additive identity is 0 and for $|n| \neq 1$, the multiplicative identity is 1.

Example 1.12 (Ring of endomorphisms)**.** Let G be an additive abelian group and set

$$\operatorname{End}(G) := \{\text{homomorphisms } G \to G\}.$$

Then the following hold:

(i) We can define the operations on $\mathrm{End}(G)$ as

$$(\phi+\psi)(x) := \phi(x)+\psi(x), \text{ and}$$
$$(\phi\psi)(x) := \phi(\psi(x)).$$

(ii) These make $\mathrm{End}(G)$ a ring with identity wherein 0, 1 and negations are given by

$$0(x) = 0,$$
$$1(x) = x, \text{ and}$$
$$(-\phi(x)) = -(\phi(x)).$$

(iii) $\mathrm{End}(G)$ is commutative $\iff$ $|G| \le 2$.

Example 1.13 (Ring of matrices)**.** Let R be a ring and $n \ge 1$. Then the set $M_{n\times n}(R)$, of $n \times n$ matrices over R, forms a ring under the usual matrix operations.

In this ring, 0 is the null matrix and additive inverses of matrices are given by entry-wise negation.

Also, the following hold:

(i) R has identity $\implies$ $R^{n\times n}$ has identity too, which is given by the usual identity matrix.

(ii) $R^{n\times n}$ has an identity $\implies$ R has an identity.

(iii) $M_{n\times n}(R)$ is commutative $\iff$ either R is the zero ring, or $n = 1$ with R commutative.

Example 1.14 (Alternate ring structure on $\mathbb{Z}$)**.** $\mathbb{Z}$ forms a commutative ring with identity under the following operations:

$$m \oplus n := m+n-1$$
$$m \odot n := m+n-mn$$

The additive and multiplicative identities here are 1 and 0 respectively.

2 Rings of polynomials

October 12, 2022

Remark. *In this section, fix R to be a ring and $n \ge 0$.*

Definition 2.1 (The set $R[x_1, \ldots, x_n]$)**.** We define $R[x_1, \ldots, x_n]$ to be the set of all functions $p\colon \mathbb{N}^n \to R$ such that $p_\alpha \neq 0_R$ for only finitely many α's in $\mathbb{N}^n$.

We'll call such functions as *polynomials*.

Proposition 2.2 ($(R[x_1, \ldots, x_n], +)$ forms a group)**.** *We can define a binary operation on $R[x_1, \ldots, x_n]$ by component-wise addition. This makes $R[x_1, \ldots, x_n]$ into an abelian group with identity and inverses given by*

$$0_\alpha = 0_R, \text{ and}$$
$$(-p)_\alpha = -(p_\alpha).$$

Definition 2.3 (Degrees and sums of indices)**.** For $\alpha, \beta \in \mathbb{N}^n$, we define $|\alpha| \in \mathbb{N}$ and $\alpha + \beta \in \mathbb{N}^n$ as

$$|\alpha| := \sum_{i=1}^{n} \alpha_i, \text{ and}$$
$$(\alpha + \beta)_i := \alpha_i + \beta_i.$$

Proposition 2.4 (Properties of indices and degrees)**.**

(i) Let $\alpha, \beta \in \mathbb{N}^n$. Then
$$|\alpha + \beta| = |\alpha| + |\beta|.$$

(ii) Let $N \in \mathbb{N}$. Then there are only finitely many α's in $\mathbb{N}^n$ such that
$$|\alpha| < N.$$

Definition 2.5 (Degree of nonzero polynomials)**.** Let $p \in R[x_1, \ldots, x_n]$ be nonzero. Then we define
$$\deg p := \max_{\substack{\alpha \in \mathbb{N}^n: \\ p_\alpha \neq 0_R}} |\alpha|.$$

Remark. *Thus degree of the zero polynomial is left undefined.*

Proposition 2.6 (Multiplication of polynomials)**.** *Let $p, q \in R[x_1, \ldots, x_n]$. Then for each $\alpha \in \mathbb{N}^n$, there are only finitely many pairs $(\beta, \gamma) \in \mathbb{N}^n \times \mathbb{N}^n$ such that $\beta + \gamma = \alpha$.*

Thus we can define $p\colon \mathbb{N}^n \to R$ as

$$(pq)_\alpha := \sum_{\substack{\beta, \gamma \in \mathbb{N}^n: \\ \beta + \gamma = \alpha}} p_\beta q_\gamma.$$

Then $p_\alpha = 0$ whenever $|\alpha| > \deg p + \deg q$ for $p, q \neq 0$, and hence $p \in R[x_1, \ldots, x_n]$.

Definition 2.7 (Monomials in multi-index notation)**.** Let $a \in R$ and $\alpha \in \mathbb{N}^n$. Then we define the polynomial $ax^\alpha \in R[x_1, \dots, x_n]$ as

$$(ax^\alpha)_\beta := a\delta_{\alpha\beta}.$$

We call polynomials of such forms as *monomials*, and if we further have $a = 1_R$, then we call this a *monic monomial*.

Proposition 2.8 (Polynomials as sums of monomials)**.** *Let* $p \in R[x_1, \dots, x_n]$. *Then*

$$p = \sum_{\substack{\alpha \in \mathbb{N}^n: \\ p_\alpha \neq 0_R}} p_\alpha x^\alpha.$$

Theorem 2.9. $R[x_1, \dots, x_n]$ *forms a ring under the above operations.*

Proposition 2.10.

(i) R *is commutative* $\iff$ $R[x_1, \dots, x_n]$ *is commutative.*

(ii) 1_R *is the identity in* R $\implies$ $1_R x^{(0,\dots,0)}$ *is the identity in* $R[x_1, \dots, x_n]$.

(iii) $R[x_1, \dots, x_n]$ *has an identity* $\implies$ R *has an identity.*

3 Idempotents, nilpotents, zero divisors...

October 13, 2022

Definition 3.1 (Idempotents, nilpotents, zero divisors)**.** Let R be a ring. Then an $x \in R$ is called

(i) *idempotent* iff $x^2 = x$;

(ii) *nilpotent* iff $x^n = 0_R$ for some $n \geq 1$; and

(iii) a *zero divisor* iff $xy = 0_R$ or $yx = 0_R$ for some $y \in R \setminus \{0_R\}$.

Example 3.2 (One-sided zero divisor)**.** Let G be an abelian group. Then in the ring $\mathrm{End}(G^\mathbb{N})$, the "left-shift" function

$$(x_1, x_2, \dots) \mapsto (x_2, x_3, \dots)$$

is a left-sided zero divisor.

Definition 3.3 (Boolean rings)**.** A ring in which each element is idempotent is called a Boolean ring.

Proposition 3.4. *Let R be a Boolean ring. Then*

(i) $-x = x$, *and*

(ii) $xy = yx$.

Example 3.5. Let X be a set. Then $(2^X, \Delta, \cap)$ forms a Boolean ring with $1 = X$.

Definition 3.6 (Cancellation property)**.** A ring R is said to obey *left-cancellation property* iff

$$ab = ac \text{ and } a \neq 0_R \implies b = c.$$

Similarly, there is *right-cancellation property.*

Proposition 3.7 (Characterizing "no nonzero divisors")**.** *Let R be a ring. Then the following are equivalent:*

(i) R has no nonzero zero divisors.

(ii) R obeys left-cancellation.

(iii) R obeys right-cancellation.

(iv) $ab = 0_R \implies a = 0_R$ *or* $b = 0_R$.

Corollary 3.8 (Further characterization of the zero ring)**.** *Let R be a ring. Then 0_R is a zero divisor* $\iff R \neq \{0_R\}$.

Theorem 3.9. *Let R be a nonzero ring with identity such that it has no nonzero zero divisor. Then the following hold:*

(i) $\operatorname{char} R = 0$ *or* $\operatorname{char} R$ *is prime.*

(ii) R is finite $\implies |R|$ *is some power of* $\operatorname{char} R$.

Result 3.10 (On idempotents)**.**

(i) A ring with identity having no nonzero zero divisors has 0 and 1 as its only idempotents.

(ii) In a commutative ring, sum of nilpotents is a nilpotent.

(iii) In a ring with identity, if a is nilpotent, then $1 \pm a$ are invertible.

4 Subrings

October 22, 2022

Definition 4.1 (Subrings)**.** Let R be a ring. The a subset $S \subseteq R$ is called a subring of R iff the operations of R can be inherited to S and S forms a ring under those inherited operations.

Proposition 4.2 (Characterizing subrings)**.** *Let R be a ring and $S \subseteq R$. Then the following are equivalent:*

(i) S is a subring of R.

(ii) $S \neq \emptyset$, and $S - S, SS \subseteq S$.

Remark. *We'll define the addition and multiplication of subsets of a ring in the obvious manner.*

Result 4.3 (The identities of the ring and subring need not be same!)**.** Let R be a ring and $e \in R$ be idempotent. Define

$$S := \{a \in R : ea = a = ae\}.$$

Then S is the largest subring of R that has identity e. Also,

$$S = eRe.$$

Example 4.4. $\{0, 3\}$ and $\{0, 2, 4\}$ are subrings of $\mathbb{Z}_6$ with identities respectively 3 and 4.

Proposition 4.5.

(i) Subrings of subrings are subrings of the parent ring.

(ii) Nonempty intersections of subrings is a subring of the parent ring.

Proposition 4.6. *Let S, T be subrings of a ring R such that $T \subseteq S$. Then T is a subring of S.*

Proposition 4.7. *Let R be a ring and $a \in R$. Then aR and Ra are subrings of R.*

Example 4.8 (Sum of subrings needn't be subrings!). Take $R := \mathbb{Q}[x]$. Then

$$S := \{a_0 + a_2x^2 + \cdots + a_{2n}x^{2n} : a_{2i} \in \mathbb{Q}\}, \text{ and}$$
$$T := \{a_0 + a_3x^3 + \cdots + a_{3n}x^{3n} : a_{3i} \in \mathbb{Q}\}$$

are subrings of R.

But $S + T$ is not closed under multiplication: $x^2\, x^3 = x^5 \notin S + T$.

Remark. *See*

Proposition 4.9 (Centers of rings). *Let R be a ring. Then the set*

$$C := \{a \in R : ax = xa \text{ for all } x \in R\}$$

is a subring of R.

Notation. *We call elements of C being "central" in R.*

Result 4.10. Monic monomials are central in the rings of polynomials.

5 Integral domains, division rings, fields, ...

October 21, 2022

Definition 5.1 (Integral domains). A ring R is called an integral domain iff the following hold:

(i) $R \neq \{0\}$.

(ii) R has an identity.

(iii) R is commutative.

(iv) R has no nonzero zero divisors.

Corollary 5.2. *Characteristic of integral domains is either 0 or it is prime.*

Theorem 5.3. *Let $n \in \mathbb{Z}$. Then $\mathbb{Z}_n$ is an integral domain $\iff$ $n = 0$ or n is prime.*

Definition 5.4 (Division rings). A ring R is called a division ring iff the following hold:

(i) $R \neq \{0\}$.
(ii) R has an identity.
(iii) Nonzero elements are invertible.

Example 5.5 (Quaternions in disguise)**.** The set

$$\left\{ \begin{bmatrix} x & y \\ -\overline{y} & \overline{x} \end{bmatrix} : x, y \in \mathbb{C} \right\}$$

forms a non-commutative division ring under the usual matrix operations.

Proposition 5.6. *Division rings have no nonzero zero divisors.*

Proposition 5.7 (Multiplicative group of a division ring)**.** *Let R be a division ring. The the multiplication can be inherited to $R \setminus \{0_R\}$ making it a group with identity 1_R and inverses given by the multiplicative inverses in R.*

Definition 5.8 (Fields)**.** Commutative division rings are called fields.

Corollary 5.9. *Fields are integral domains.*

Theorem 5.10. *Finite nontrivial rings with no nonzero zero divisors are division rings.*

Corollary 5.11. *Finite integral domains are fields.*

Corollary 5.12. *Let $p \in \mathbb{Z}$. Then $\mathbb{Z}_p$ is a field $\iff$ p is prime.*

Definition 5.13 (Subfields)**.** Let F be a field. Then a subset $K \subseteq F$ is called a subfield of F iff the operations of F can be inherited to K and K forms a field under these operations.

Proposition 5.14 (Characterizing subfields)**.** *Let F be a field and $K \subseteq F$. Then the following are equivalent:*

(i) K *is a subfield of* F.
(ii) $|K| \geq 2$, *and* $K - K \subseteq K$ *and* $K(K \setminus \{0_F\})^{-1} \subseteq K$.

6 Ideals

October 23, 2022

Definition 6.1 (Ideals)**.** Let R be a ring. Then a subring I of R is called an ideal iff

$$IR, RI \subseteq I.$$

Remark. *If $RI \subseteq I$, then I is called the* "left ideal"*, and if $IR \subseteq I$, then I is called the* "right ideal"*.*

Example 6.2 (One-sided ideals)**.** Let R be a ring. Then the set

$$\left\{ \begin{bmatrix} x & 0_R \\ y & 0_R \end{bmatrix} : x, y \in R \right\}$$

is a left ideal.

Corollary 6.3 (Characterizing an ideal)**.** *Let R be a ring and $I \subseteq R$. Then the following are equivalent:*

(i) I is an ideal of R.

(ii) $I \neq \emptyset$, and $I - I, RI, IR \subseteq I$.

Proposition 6.4. *Nonempty intersections of ideals are ideals.*

Proposition 6.5 (nR's are ideals)**.** *Let R be a ring and $n \in \mathbb{R}$. Then*

$$nR := \{nr : r \in R\}$$

is an ideal of R.

Example 6.6 (Ideal of an ideal needn't be an ideal)**.** Consider $\mathbb{Q}[x]$. Then $x\,\mathbb{Q}[x]$ is an ideal of $Q[x]$ (see Corollary 7.3). Now, $\{a_1x + a_2x^2 + \cdots + a_nx^n : a_1 \in \mathbb{Z}\}$ is an ideal of $x\,\mathbb{Q}[x]$, but not of $\mathbb{Q}[x]$.

Proposition 6.7 (Subring + ideal = subring)**.** *Let S be a subring of a ring R and I be an ideal. Then $S + I$ is a subring of R.*

Example 6.8 (Subring + ideal $\neq$ ideal!)**.** Let $R := \mathbb{Q}[x]$. Then

$$\begin{aligned} &S := \{a_0 + a_2x^2 + \cdots + a_{2n}x^{2n} : a_{2i} \in \mathbb{Q}\}, \text{ and} \\ &I := x^2\,\mathbb{Q}[x] \end{aligned}$$

are respectively a subring and an ideal of R (see Corollary 7.3). But

$$S + I = \{a_0 + \cdots + a_nx^n : a_1 = 0\}$$

is not an ideal since $x \in R(S + I)$ but $x \notin S + I$.

Definition 6.9 ("Ideal" product of subsets of rings)**.** Let R be a ring and $A, B \subseteq R$. Then we define

$$A \cdot B := \{\text{finite sums in } AB\}.$$

Remark. *We could have alternatively viewed it as $\sum_{i=1}^{\infty} AB$. But let's be lazy to not formalize arbitrary sums or products of sets in a ring.*

Definition 6.10 (Ideals generated by subsets)**.** Let R be a ring and $S \subseteq R$. Then we define

$$(\!|S|\!) := \text{the smallest ideal in } R \text{ that contains } S.$$

Theorem 6.11 (Sums and products of ideals are ideals)**.** *Let I, J be ideals of a ring. Then the following hold:*

(i) $I + J = (\!|I \cup J|\!)$.

(ii) $I \cdot J = (\!|IJ|\!) \subseteq I \cap J$.

Proposition 6.12 (Principal ideals)**.** *Let R be a ring and $a \in R$. Then*

$$(\!|a|\!) = \left\{ na + ra + \sum_{i=1}^{m} r_i a s_i + as : m, n \in \mathbb{Z}, m \geq 0, r, r_1, \ldots, r_m, s, s_1, \ldots, s_m \in R \right\}.$$

If R is commutative, then this simplifies to

$$(\!|a|\!) = \left\{ na + ra : n \in \mathbb{Z}, r \in R \right\}.$$

If R has identity, then we have

$$(\!|a|\!) = \left\{ \sum_{i=1}^{m} r_i a s_i : m \geq 0, r_1, \ldots, r_m, s_1, \ldots, s_m \in R \right\}.$$

If R is both commutative and has identity, then we simply have

$$Ra = (\!|a|\!) = aR.$$

Definition 6.13 (Principal ideal rings and domains)**.** Let R be a ring. Then ideals of the form $(\!|a|\!)$ are called *principal*.

If R's ideals are all principal, then it's called a *principal ideal ring*. If R is an integral domain too, then we call it a *principal ideal domain*.

Example 6.14.

(i) $2\mathbb{Z}$ is a principal ideal ring, but not an integral domain.

(ii) $\mathbb{Z}[x]$ has non-principal ideals like $(\!|2, x^2|\!)$.

Definition 6.15 (Simple rings)**.** Nontrivial rings with no nontrivial ideals are called simple.

Proposition 6.16. *Division rings are simple.*

Proposition 6.17. *Simple commutative rings with identity are fields.*

7 Studying aR and Ra's

October 24, 2022

Proposition 7.1 (Ideals via central elements)**.** *Let R be a ring and $a \in R$. Then we have the following implications:*

$$a \text{ is central} \implies aR = Ra \implies aR, Ra \text{ are ideals}$$

If R has an identity, the the converse of the last implication is true.

Example 7.2 (The converses are false!)**.**

(i) For the first implication: Take $R := \mathbb{R}^{2\times 2}$ and a to be any non-commutative invertible matrix.

(ii) Take $R := \left\{ \left[\begin{smallmatrix} x & 0 \\ y & 0 \end{smallmatrix}\right] : x, y \in \mathbb{R} \right\}$ (which is a left ideal of $\mathbb{R}^{2\times 2}$) and $a := \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$.

(iii) See this.

Corollary 7.3. *Let R be a ring and $n \geq 0$. Let $m \in R[x_1, \ldots, x_n]$ be a monic monomial. Then $mR = Rm$ is an ideal of $R[x_1, \ldots, x_n]$.*

Definition 7.4 (Ideals generated by a set)**.** Let R be a ring and $S \subseteq R$. Then we define

$$(\!|S|\!) := \text{smallest ideal of } R \text{ containing } S.$$

Proposition 7.5 ($(\!|a|\!)$ and aR)**.** *Let R be a ring and $a \in R$. Then*

$$(\!|a|\!) \supseteq aR + Ra \supseteq (\!|aR|\!), (\!|Ra|\!).$$

If R has identity, then the above become equalities.

Example 7.6. For $R := x\,\mathbb{Q}[x]$ and $a := x$, we have $(\!|a|\!) \supsetneq Ra = aR$.

8 Quotient rings

October 31, 2022

Proposition 8.1 (Quotient rings)**.** *Let R be a ring with an ideal I. Then the binary operations on R/I*

$$\begin{aligned} +\colon (\bar{a}, \bar{b}) &\mapsto \overline{a+b}, \text{ and} \\ \text{juxtapositive product}\colon (\bar{a}, \bar{b}) &\mapsto \overline{ab} \end{aligned}$$

are well-defined and make R/I a ring with $0_{R/I} = \overline{0_R}$.

9 Ring homomorphisms

November 23, 2022

Definition 9.1 (Ring homomorphism)**.** Let R, S be rings. Then a function $\phi\colon R \to S$ is called a ring homomorphism iff

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b), \text{ and} \\ \phi(ab) &= \phi(a)\,\phi(b). \end{aligned}$$

Corollary 9.2.

(i) For an ideal I of a ring R, the canonical function $R \to R/I$ is a ring homomorphism.

(ii) Compositions of ring homomorphisms are ring homomorphism.

(iii) Restrictions of ring homomorphisms to subrings of domain and codomain are ring homomorphisms.

(iv) Identity map on a ring is a ring homomorphism.

Remark. *"$\phi\colon R \to S$ is a ring homomorphism" will be taken to also imply that R, S are rings.*

Proposition 9.3 (Properties of ring homomorphisms)**.** *Let $\phi\colon R \to S$ be a ring homomorphism. Then the following hold:*

(i) $\phi(0_R) = 0_S$.

(ii) $\phi(-a) = -\phi(a)$.

(iii) $\phi(na) = n\phi(a)$ *for* $n \in \mathbb{Z}$.

(iv) $\phi(a^n) = \phi(a)^n$ *for* $n \geq 1$.

(v) $\phi(R)$ *is a subring of* S.

(vi) Let R have identity. Then the following hold:

  (a) $\phi(1_R)$ *is the identity of* $\phi(R)$.

  (b) $\phi(a^n) = \phi(a)^n$ *for* $n \geq 0$.

  (c) $a \in R$ *is invertible* $\implies$ $\phi(a) \in \phi(R)$ *is invertible in with* $\phi(a^n) = \phi(a)^n$ *for each* $n \in \mathbb{Z}$.

Proposition 9.4 (Preservations under ring homomorphisms)**.** *Under a ring homomorphism,*

(i) subrings are preserved both ways,

(ii) ideals are preserved in the backward direction, and

(iii) commutativity is preserved in the forward direction.

Definition 9.5 (Kernel)**.** For a ring homomorphism $\phi\colon R \to S$, we define

$$\ker \phi := \phi^{-1}(\{0_S\}).$$

Corollary 9.6.

(i) Kernel of a ring homomorphism is an ideal of the domain ring.

(ii) A ring homomorphism is injective $\iff$ *its kernel is the zero ideal.*

Definition 9.7 (Ring isomorphisms)**.** A ring isomorphism is a bijective ring homomorphism.

A ring R is said to be *isomorphic* to S iff there exists a ring isomorphism $R \to S$.

Proposition 9.8. *The inverse of a ring isomorphism is a ring homomorphism.*

Proposition 9.9. *"Being isomorphic" is an equivalence relation for rings.*

Notation. *As before, we'll denote this congruence by "$\cong$".*

Theorem 9.10 (First isomorphism)**.** *Let $\phi\colon R \to S$ be a surjective ring homomorphism. Then*

$$R/\ker\phi \cong S.$$

Theorem 9.11 (Second isomorphism)**.** *Let I be an ideal and S be a subring of a ring R. Then*[3]

$$\frac{S}{I \cap S} \cong \frac{I+S}{I}.$$

Theorem 9.12 (Third isomorphism)**.** *Let I, J be ideals of a ring R with $I \subseteq J$. Then*

$$\frac{R/I}{J/I} = \frac{R}{J}.$$

Theorem 9.13 (Correspondence)**.** *Let $\phi\colon R \to S$ be a surjective ring homomorphism. Then we have the following one-to-one correspondence:*

$$\begin{array}{ccc} \{\textit{ideals of } R \textit{ containing } \ker\phi\} & \longleftrightarrow & \{\textit{ideals of } S\} \\ I & & \phi(I) \\ \phi^{-1}(J) & & J \end{array}$$

10 Maximal and prime ideals

November 23, 2022

Definition 10.1 (Maximal and prime ideals)**.** A proper ideal I of a ring R is said to be

(i) *maximal* iff the only ideal properly containing it is R itself; and,

(ii) *prime* iff the following holds: $ab \in I \implies a \in I$ or $b \in I$.

Proposition 10.2.

(i) Maximal ideals of $\mathbb{Z}$ are precisely $p\mathbb{Z}$ for prime p's.

(ii) Prime ideals of $\mathbb{Z}$ are precisely $n\mathbb{Z}$ where $n = 0$ or n is prime.

[3] As before, when we'll quotient a ring with a subset, we'll omit mentioning that the subset is an ideal.

Theorem 10.3 (Characterizing fields and integral domains)**.** *Let R be a commutative ring with identity. Then the following hold:*

(i) R is a field $\iff$ $\{0_R\}$ is a maximal ideal.

(ii) R is an integral domain $\iff$ $\{0_R\}$ is a prime ideal.

Further, if I is an ideal of R, then the following hold:

(i) R/I is a field $\iff$ I is maximal.

(ii) R/I is an integral domain $\iff$ I is prime.

Theorem 10.4. *In a commutative ring with identity, maximal ideals are prime.*

Example 10.5 (A non-maximal prime)**.** Consider $0\mathbb{Z} \times 2\mathbb{Z}$ in $\mathbb{Z} \times \mathbb{Z}$.

Proposition 10.6 (When can primes be maximal?)**.**

(i) In a principal ideal domain, nonzero prime ideals are maximal.

(ii) In a Boolean ring with identity, prime ideals are maximal.

11 Embedding rings in larger rings

November 23, 2022

Lemma 11.1. *Let R be a ring and $k := \operatorname{char} R$. Then the following hold:*

(i) $\mathbb{Z} \times R$ forms a ring under the following operations:

$$\begin{aligned} (m, a) + (n, b) &:= (m + n,\ a + b) \\ (m, a)\,(n, b) &:= (mn,\ mb + na + ab) \end{aligned}$$

(ii) $\mathbb{Z}_k \times R$ forms a ring with the following well-defined operations:

$$\begin{aligned} (m, a) + (n, b) &:= \big((m + n) \bmod k,\ a + b\big) \\ (m, a)\,(n, b) &:= \big((mn) \bmod k,\ mb + na + ab\big) \end{aligned}$$

Theorem 11.2. *Let R be a (commutative) ring. Then there exists a (commutative) ring S with identity, having $\operatorname{char} S = 0$,[4] which contains a copy[5] of R as an ideal.*

[4]Instead, we can also have $\operatorname{char} S = \operatorname{char} R$.

[5]That is, an isomorphic image

Theorem 11.3 (Field of fractions)**.** *Let R be an integral domain. Then the relation on $R \times R \setminus \{0_R\}$ defined by*

$$(a, b) \sim (c, d) \text{ iff } ad = bc$$

is an equivalence relation, whose equivalence classes form a field under the following well-defined operations:

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

Further, this field of fractions of R *contains a copy of R via* $a \mapsto [(a, 1_R)]$*.*

Theorem 11.4. *Let F be a field and $R \subseteq F$ form an integral domain under the inherited operations.*[6] *Then*

$$\{ab^{-1} : a, b \in R, b \neq 0_F\}$$

is the smallest subfield of F that contains R. It is further isomorphic to the field of fractions of R.

Corollary 11.5. *Any field containing a copy of an integral domain also contains a copy of its field of fractions.*

12 Factorizations

November 24, 2022

Definition 12.1 (Divisors and associates)**.** Let R be a commutative ring and $a, b \in R$. Then we say

(i) that *a divides b* or *a is a divisor of b*, written $a \mid b$, iff $b = ac$ for some $c \in R$; and,

(ii) that *a and b are associates*, written $a \sim b$, iff $a \mid b$ and $b \mid a$.

Corollary 12.2. *In commutative rings, being a divisor is a transitive relation, and being associates is an equivalence relation.*

Proposition 12.3 (Properties when we also have identity)**.** *Let R be a commutative ring with identity and $a, b, u \in R$. Then the following hold:*

[6] Implicit is the fact that the operations can in the first place be inherited.

(i) $a \mid b \iff b \in (\!|a|\!) \iff (\!|b|\!) \subseteq (\!|a|\!)$.

(ii) $a \sim b \iff (\!|a|\!) = (\!|b|\!)$.

(iii) u *is invertible* $\iff u \sim 1_R \iff (\!|u|\!) = R$.

(iv) *If* R *has no nonzero zero divisors, then* $a \sim b \iff b = av$ *for some invertible* $v \in R$.

Definition 12.4 (Primes and irreducibles)**.** Let R be a commutative ring. Then a nonzero non-invertible $a \in R$ is called

(i) *prime* iff $a \mid bc \implies a \mid b$ or $a \mid c$.

(ii) *irreducible* iff a doesn't factor into two non-invertibles.

Proposition 12.5 (Properties when we also have identity)**.** *Let* R *be a commutative ring with identity and* $a \in R$ *be nonzero and non-invertible. Then the following hold:*

(i) a *is prime* $\iff (\!|a|\!)$ *is a nonzero prime ideal.*

(ii) a *is irreducible* $\implies$ *only divisors of* a *are invertibles and associates of* a.

(iii) If R *further has no nonzero zero divisors, then the following hold:*

(a) Converse of (ii).

(b) a *is prime or* $(\!|a|\!)$ *is maximal* $\implies a$ *is irreducible.*

Theorem 12.6 (Primes and irreducibles coincide in PID's)**.** *Let* R *be a principal ideal domain and* $a \in R$*. Then the following are equivalent:*

(i) a *is prime.*

(ii) $(\!|a|\!)$ *is nonzero prime.*

(iii) $(\!|a|\!)$ *is maximal.*

(iv) a *is irreducible.*