Groups, Rings and Fields

Thobias Høivik

Spring 2026

Contents

1 Groups

Definition 1.1 (Group). *A group is a set S together with a binary operation $\circ$ such that the following properties hold:*

1. *Identity: There exists an element $e \in S$, satisfying*

$$e \circ a = a \circ e = a$$

   for every $a \in S$.

2. *Inverses: For every $a \in S$ there exists $b \in S$ such that*

$$a \circ b = b \circ a = e, \text{ the identity element}$$

   We usually denote this element as a^{-1} or $-a$, depending on context.

3. *Associativity: For any $a, b, c \in S$, we require*

$$a \circ (b \circ c) = (a \circ b) \circ c$$

A group is then the tupple $(S, \circ)$. We will often just write the set to refer to the group, e.g. refering to the group $(\mathbb{Z}, +)$ as just $\mathbb{Z}$.

1.1 Basic Examples

Example 1.1 (Integers under addition). *The set of integers $\mathbb{Z}$ with the operation $+$ forms a group:*

- *Identity: 0 since $0 + n = n + 0 = n$ for all $n \in \mathbb{Z}$.*
- *Inverses: For $n \in \mathbb{Z}$, the inverse is $-n$.*
- *Associativity: Addition is associative.*

Hence $(\mathbb{Z}, +)$ is a group.

Example 1.2 (Non-example: Natural numbers under addition). *The set $\mathbb{N}$ under $+$ is* not *a group since there is no inverse for $n > 0$.*

1.2 Basic Properties

Theorem 1.1 (Uniqueness of identity). *The identity element in a group is unique.*

Proof. Suppose e and e' are both identities. Then

$$e = e \circ e' = e',$$

so the identity is unique. □

Theorem 1.2 (Uniqueness of inverses). *Each element in a group has a unique inverse.*

Proof. Suppose b and c are inverses of a. Then

$$b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c.$$

□

1.3 Example Problem

Problem 1.1. *Determine whether the set*

$$G = \{1, -1, i, -i\} \subset \mathbb{C}$$

with multiplication is a group.

Solution. We check the group axioms:

1. **Closure:** Multiplying any two elements of G yields another element in G. True.
2. **Identity:** The element 1 acts as identity. True.
3. **Inverses:** Each element has an inverse in G: $1^{-1} = 1$, $(-1)^{-1} = -1$, $i^{-1} = -i$, $(-i)^{-1} = i$. True.
4. **Associativity:** Multiplication of complex numbers is associative. True.

Hence $(G, \cdot)$ is a group, in fact it is an abelian group which we shall describe below in definition 1.2. □

1.4 Abelian Groups

Definition 1.2 (Abelian Group). *A group $(G, \circ)$ is* abelian *(or commutative) if*

$$a \circ b = b \circ a \quad \forall a, b \in G.$$

Example 1.3. *The group $(\mathbb{Z}, +)$ is abelian because $m + n = n + m$.*

2 Important Groups

First let's define some often used notation.

For $g \in G$, define:

- $g^n = gg \dots g (n > 0)$
- $g^0 = e$
- $g^{-n} = (g^{-1})^n$

and recognize the following identities (which are provable by induction):

$$g^m g^n = g^{m+n}, \quad (g^m)^n = g^{mn}$$

Definition 2.1 (Roots of Unity).

$$U_n = \{e^{2\pi ik/n} : 0 \leq k < n\}$$

are called the n-th roots of unity.

Definition 2.2. *An subset $\{g_1, \dots, g_k\} \subseteq G$ is a generating set if every $g \in G$ can be expressed as*

$$g_1^{n_1} \cdots g_k^{n_k}$$

If a singleton g' alone generates a group then it is called a generator of G and G is said to be cyclic.

The n-th roots of unity are finite, with exactly n elements. They are cyclic, with generator $e^{2i\pi/n}$.

Definition 2.3 (Symmetric Group). *The symmetric group S_n is the set of all permutations of n elements under composition. In other words it is the set of all $\sigma : [n] \to [n]$ with composition as its operation.*

The symmetric group is non-abelian for $n \geq 3$. The identity corresponds to the identity permutation (doing nothing) and inverses are undoing a permutation. We have the following notation for permutations in the symmetric Group (assume $n = 3$ for this example):

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

corresponds to $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$.

Another way to write the same permutation is:

$$(1\,2\,3)$$

3 Subgroups

Definition 3.1 (Subgroup). *Let G be a group under $\star$. A subgroup $H \leq G$ is a subset $H \subseteq G$ that is itself a group under $\star$.*

Having to mechanically check if $H \subseteq G$ satisfies all the required axioms can be a bit tedious so next we introduce a powerful theorem which let's us easily determine whether some subset is a subgroup or not.

Theorem 3.1 (Subgroup Test). *A nonempty subset $H \subseteq G$ is a subgroup if and only if*

$$\forall x, y \in H,\ xy^{-1} \in H.$$

Proof Idea. If H is a subgroup the required conditions follows.

Conversely:

- Nonempty so some $h \in H$.
- $hh^{-1} = e \in H$.
- Closure under xy^{-1} will give inverses and closure.

□

We get some nice corollaries from this, as well as a nice and tidy way to prove whether or not a subset is a subgroup.

Corollary 3.1. *The intersection of any collection of subgroups is a subgroup.*
Given any subset $S \subseteq G$, there is a smallest subgroup containing it.

Definition 3.2 (Cyclic Subgroups). *Let G be a group.*
For any $g \in G$, define:

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

$\langle g \rangle$ is called the cyclic subgroup generated by g.

It is very straightforward to show that the cyclic subgroup generated by some $g \in G$ is indeed a subgroup with the use of theorem 3.1.

On page 6 we say that a group is cyclic if it has a signle element which generates it, but now we can simply say that a group G is cyclic if $G = \langle g \rangle$ for some $g \in G$.

Theorem 3.2. *Suppose a group G is cyclic, i.e. $G = \langle g \rangle$ for some $g \in G$.*
Then it is isomorphic to one of the following:

- $(\mathbb{Z}, +)$, *or*
- $(\mathbb{Z}/n\mathbb{Z}, +)$ *for some $n \geq 1$.*

3.1 Structure of Cyclic Subgroups

Definition 3.3 (Order). *The order of an element $g \in G$ is*

$$\mathrm{ord}(g) = |\langle g \rangle|$$

Furthermore, if $\mathrm{ord}(g) = n < \infty$, then $g^n = e$ and n is minimal, otherwise we say g has infinite order.

If $\mathrm{ord}(g) = n$, then:

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$$

Moreover:

- $g^k = e \Leftrightarrow n \mid k$
- $\langle g^k \rangle = \langle g \rangle \Leftrightarrow \gcd(k, n) = 1$

Theorem 3.3. *Every subgroup of a cyclic group is cyclic.*
More precisely:

- *Subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$.*
- *Subgroups of $\mathbb{Z}/n\mathbb{Z}$ correspond to the divisors of n.*

With all of this machinery we can approach group theory with geometric and algebraic intuition. Cyclic groups are like repeated motion, finite cyclic groups corresponding to rotations by rational angles and infinite ones corresponding to translations.

4 Cosets and Lagrange's Theorem

Definition 4.1 (Left and Right Cosets). *Let $H \leq G$, and let $g \in G$. The left- and right cosets are:*

$$gH = \{gh : h \in H\} \quad Hg = \{hg : h \in H\}$$

respectively.

A key intuition is that a coset is like a copy of H shifted by g. We may also recognize that the cosets are the same size as H by identifying $h \mapsto gh$ to be a bijection and so forth.

The next natural question is when are two cosets equal? Like with showing when a subset is a subgroup we have a little trick for this problem.

Theorem 4.1. *Let G be a group.*
For $g_1, g_2 \in G$, the following are equivalent:

$$\begin{gathered} g_1 H = g_2 H \\ \Updownarrow \\ g_2^{-1} g_1 \in H \\ \Updownarrow \\ g_1 \in g_2 H \end{gathered}$$

Theorem 4.2. *The set of all left cosets of $H \leq G$ forms a partition of G.*
That is,

- *Every element of G is in exactly on coset.*
- *Two cosets are either the same or disjoint.*

Definition 4.2. *Let G be a group with $H \leq G$.*
The index of H in G, written $[G : H]$, is the number of left cosets of H.

If G is finite we get $|G| = [G : H] \cdot |H|$.

Theorem 4.3 (Lagrange's Theorem). *Let G be a group with $H \leq G$. Then:*

$$|H| \,\big|\, |G|$$

Proof. Let G be a group with $H \leq G$.

Recall that by theorem 4.2 we have that the set of left cosets of H, $g_1H, g_2H, \ldots, g_kH$ (this set is finite since G is finite) are pairwise disjoint, satisfying

$$G = \bigcup_{i=1}^{k} g_iH$$

meaning

$$|G| = \sum_{i=1}^{k} |g_iH|$$

Recall also that $|H| = |g_iH|, \forall i \in [k]$. Thus

$$|G| = \sum_{i=1}^{k} |H| = k|H|$$

In other words $|G|$ is $|H|$ times some integer k, therefore $|H|$ divides $|G|$. □

Theorem 4.3 has the following immediate consequences:

- The order of any element divides $|G|$.
- $g^{|G|} = e$ for every $g \in G$.

Beware that it does not follow from Lagrange's Theorem that there exists a subgroup with the order of a divisor of $|G|$ for every divisor of G. The alternating group of order 12, A_4, has no subgroup of order 6 for example.

Proposition 4.1. *A group of order p where p is prime, is cyclic.*

Proof Sketch. Let G be a group with $|G| = p$ (prime).

Let $g \in G \setminus \{1\}$. Consider it's generated subgroup $\langle g \rangle$. By Lagrange's Theorem the order of this subgroup divides p so $|\langle g \rangle|$ is 1 or p, but it can't be 1 as $g \neq 1$ so it's order is p, i.e. g generates the entirety of G. □

4.1 Problems relating to subgroups

Problem 4.1. *Let G be a group and $g \in G$ with ord$(g) = 12$.*

- *List all distinct subgroups of $\langle g \rangle$.*
- *For which integers k does g^k generate $\langle g \rangle$?*

Solution. Recalling that $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$, we want to find all the distinct subgroups of $\langle g \rangle$. In other words, which subsets of $\langle g \rangle$ are also groups with respect to the operation of G?

ord$(g) = |\langle g \rangle| = 12$ hence $\langle g \rangle = \{g^0, g^1, \dots, g^{11}\}$. We know that there are two trivial subgroups of $\langle g \rangle$, namely $\{g^0\}$ and $\langle g \rangle$. Otherwise, we know that every cyclic subgroub of a cyclic group (which $\langle g \rangle$ is) is itself cyclic, so we can find the subgroups by looking at the generated groups of each element of $\langle g \rangle$. Otherwise, we could use the fact that $\langle g \rangle$ is isomorphic to $\mathbb{Z}/12\mathbb{Z}$ together with realizing that the number of subgroups is then the same as the number of positive divisors of 12.

Using the first approach we get:

$$\begin{aligned}
\langle g^2 \rangle &= \{g^n : n = 2k,\ k \in \mathbb{Z}\} \\
&= \{e, g^2, \dots, g^10\} = \langle g^10 \rangle \\
\langle g^3 \rangle &= \{e, g^3, g^6, g^9\} = \langle g^9 \rangle \\
\langle g^4 \rangle &= \{e, g^4, g^8\} = \langle g^8 \rangle \\
\langle g^6 \rangle &= \{e, g^6\}
\end{aligned}$$

Those integers which are coprime to 12, like $1, 5, 7, 11$, will generate $\langle g \rangle$. Thus we have 6 distinct subgroups, exactly the same as the number of positive divisors of 12, as expected. □

Problem 4.2. *Let G be any group $H = \langle g \rangle$ where ord$(g) < \infty$. Prove that if $g^m \in H$, then $\langle g^m \rangle \leq H$.*

Proof. Assume, for contradiction, that $g^m \in H$, but $\langle g^m \rangle$ is not a subgroup of H.

Let $s = m \mod \text{ord}(g)$. Then $\langle g^m \rangle = \{g^{sk} : k \in \mathbb{Z}\} \neq \emptyset$. It is clear that this is a subset of $\langle g \rangle = H$, since $\langle g \rangle$ is closed under the group operation and $g^m \in H$. Then the only way our assumption is true is if there exists some $x, y \in \langle g^m \rangle$ such that $xy^{-1} \notin \langle g^m \rangle$.

Every element $x, y \in \langle g^m \rangle$ is of the form $x = g^{sn}, y = g^{st}$ for some $n, l \in \mathbb{N}$. By assumption, $xy^{-1} = g^{s(n-t)} \notin \langle g^m \rangle$ which would necessarily mean that $n - t \notin \mathbb{Z}$, impossible. □

The above argument can be made more rigorous by considering the isomorphism between $\langle g^m \rangle$ and $\mathbb{Z}/s\mathbb{Z}$, or by proving the claim directly (I am an idiot, and this was a bad approach).

5 Normal subgroups

Definition 5.1 (Normal subgroup). *A subgroup $H \leq G$ is normal, written $H \trianglelefteq G$, if:*

$$gH = Hg, \forall g \in G$$

with the equivalent characterization:

$$H \trianglelefteq G \Leftrightarrow gHg^{-1} = H, \forall g \in G$$

A few things to tick off immediately;

1. Every subgroup of an abelian group is normal.
2. {e} and G are always normal.
3. The alternating group $A_n \trianglelefteq S_n$.
4. Subgroups of index 2 are always normal.

If you consider the map (conjugation)

$$x \mapsto gxg^{-1},$$

which constitutes an automorphism of G we can say the following.

Normal subgroups are precisely those subgroups which are fixed under every conjugation.

Definition 5.2 (Quotient Group). *If $H \trianglelefteq G$, define:*

$$G/H := \{gH : g \in G\}$$

with an operation we'll call multiplication by:

$$(gH)(kH) = (gk)H$$

Theorem 5.1. *The quotient group with multiplication, as defined above, is a well-defined group.*

Definition 5.3. *We define the* ***canonical projection*** *as*

$$\pi : G \to G/H,\ \pi(g) = gH.$$

Notably, the projection π constitutes a homomorphism with kernel $\ker \pi = H$. Notice that this claim of the kernel being H itself should be immediately obvious as hH for some $h \in H$ is itself H as it's closed.

6 Exercises for Week 1

Problem 6.1 (29, p.48). *Show that if G is a finite group with identity e and an even number of elements, then there is $a \neq e$ in the group such that $a * a = e$.*

Proof. We are being asked to show that in a finite group with even order, there exists some element other than the identity which is it's own inverse.

Recall uniqueness of inverses and that for $g \in G$, $(g^{-1})^{-1} = g$. Thus for every element there exists one and only one element which is it's inverse. $e^{-1} = e$ is covered. In $G \setminus \{e\}$ there are an odd number of elements. Each of these have exactly one unique inverse meaning that there is one element "left" over which then necessarily has itself as it's inverse. □

Problem 6.2 (33, p.49). *Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a proof by mathematical induction that $(a * b)^n = a^n * b^n$ for all $a, b \in G$.*

Proof. Let $a, b \in G$. The base case where $n = 1$ is trivial so we proceed to our assumption that for any $k \in \mathbb{Z}^+$ we have $(a * b)^k = a^k * b^k$.

Let $n = k + 1$.

$$\begin{aligned}
(a * b)^n &= (a * b)^{k+1} \\
&= (a * b)^k * (a * b) \\
&= a^k * b^k * (a * b) && \text{by hypothesis} \\
&= a^k * (b^k * a) * b && \text{by associativity} \\
&= a^k * (a * b^k) * b && \text{by commutativity} \\
&= (a^k * a) * (b^k * b) \\
&= (a^{k+1}) * (b^{k+1}) \\
&= a^n * b^n
\end{aligned}$$

By the principle of mathematical induction we have that

$$(a * b)^n = a^n * b^n, \ \forall n \in \mathbb{Z}^+$$

□

Problem 6.3 (35, p. 49). *Show that if* $(a*b)^2 = a^2 * b^2$ *for* a, b *in a group, then* $a*b = b*a$.

Proof.

$$\begin{aligned}(a*b)^2 &= (a*b)*(a*b)\\ a^2*b^2 &= (a*a)*(b*b)\\ \Rightarrow (a*b)*(a*b) &= (a*a)*(b*b)\\ a*(b*a)*b &= a*(a*b)*b\end{aligned}$$

By one application each of left- and right cancellation we have

$$a*b = b*a$$

□

Problem 6.4 (41, p. 49). *Let* G *be a group and fix* $g \in G$. *Show that the map* i_g, *s.t.* $i_g(x) = gxg^{-1}$ *for* $x \in G$. *Show that* i_g *is an automorphism on* G.

Proof. Let $i_g : G \to G$ be defined as above. We need to show that it satisfies all the properties of an isomorphism.

It is clear, through left- and right cancellation, that i_g is injective.

Notice also that for any $x \in G$ we have the pre-image $g^{-1}xg$ since $i_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x$, hence i_g is surjective.

Lastly we verify the homomorphism property:

$$\begin{aligned}i_g(xy) &= gxyg^{-1}\\ &= gxeyg^{-1}\\ &= gxg^{-1}gyg^{-1}\\ &= i_g(x)i_g(y)\end{aligned}$$

completing the proof. □

7 Problems for week of Jan 26

Problem 7.1 (Problem 44 Fraleigh's p.67). *Let $G = \langle a \rangle$ be a cyclic group isomorphic to a group G'. If $\phi : G \to G'$ is an isomorphism, show that for every $x \in G$, $\phi(x)$ is uniquely determined by $\phi(a)$. That is, if ϕ and ψ constitutes isomorphisms from $G \to G'$ with $\phi(a) = \psi(a)$, then $\phi(x) = \psi(x)$ for every $x \in G$.*

Proof. Let G be generated by a, isomorphic to G' via ϕ and ψ, satisfying

$$\phi(a) = \psi(a)$$

Let $x \in G$. Then $x = a^n$ for some $n \in \mathbb{Z}$, as $G = \langle a \rangle$. Observe the following:

$$\begin{aligned} \phi(x) &= \phi(a^n) \\ &= \phi(a)^n \\ &= \psi(a)^n \\ &= \psi(a^n) = \psi(x) \end{aligned}$$

This completes the proof. □

Problem 7.2 (Problem 6 Fraleigh's p.83). *Compute $|\sigma|$ for*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$$

Solution. Observe that σ is the permutation which sends

$$\begin{aligned} 1 &\to 3 \\ 2 &\to 1 \\ &\vdots \\ 6 &\to 2 \end{aligned}$$

so σ^2 is

$$\begin{aligned} 1 &\to 4 \\ 2 &\to 3 \\ &\vdots \\ 6 &\to 1 \end{aligned}$$

We want to find $n \in \mathbb{N}$ such that $\sigma^n =$ the identity permutation. It's easy to see that performing the permutation 6 times gives $1 \to 1$ which we would require. We also see that $2 \to 2$, $3 \to 3$ and so on.

We could also write the permutation in compact form and see that σ is a cycle of length 6, so the order is 6. □

Problem 7.3 (Problem 7 Fraleigh's p.83). *Compute* $|\tau|$ *for*

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

Solution. Note that τ in compact notation is

$$\tau = (1\ 2\ 4\ 3)(5\ 6)$$

so τ is the composition of a 2- and 4-cycle.

$$|\tau| = \texttt{lcm}(4, 2) = 4$$

□

Problem 7.4 (Problem 49 Fraleigh's p.86). *If* A *is a set, then a subgroup* $H \leq S_A$ *is transitive on* A *if for each* $a, b \in A$ *there exists* $\sigma \in H$ *such that* $\sigma(a) = b$*. Show that if* A *is a nonempty finite set, then there exists a finite cylic subgroup* H *of* S_A *with* $|H| = |A|$ *that is transitive on* A*.*

Proof. Let $A = \{a_1, a_2, \ldots, a_n\}$ with S_A being the permutations on A. Let $\sigma \in S_A$ be the permutation which sends $a_i \to a_{i+1}$ (take i modulo n). It is clear that σ^k is the permutation which sends a_i to a_{i+k} and furthermore $|\sigma| = n = |A|$. It is not hard to see that $\langle \sigma \rangle$ forms a subgroup where each permutation shifts all elements of A.

It is clear that for any $a_i, a_j \in A$ we can find a permutation which sends one to the other. Suppose, without loss of generality, $i < j$. Then $\sigma^{j-i}(a_i) = a_j$, and the inverse of said permutation sends a_j to a_i.

A bit inelegantly written, but I digress. □

Problem 7.5 (Problem 1 Fraleigh's p.94). *Find the orbit of*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \end{pmatrix}$$

Solution. We are looking at $\sigma \in S_6$ acting on $[6]$ (I assume) so we want to find

$$\left\{ \texttt{Orb}_\sigma(n) = \{\sigma^k(x) : k \in \mathbb{Z}\} \mid n = 1, 2, \ldots, 6 \right\}$$

Let us rewrite σ more compactly.

$$1 \to 5 \to 2 \to 1$$

$$3 \to 3$$

$$4 \to 6 \to 4$$

so

$$\sigma = (1\ 5\ 2)(4\ 6)$$

Thus we have the following orbits:

$$\begin{aligned} \mathsf{Orb}_\sigma(1) = \mathsf{Orb}_\sigma(2) = \mathsf{Orb}_\sigma(5) &= \{1,2,5\} \\ \mathsf{Orb}_\sigma(4) = \mathsf{Orb}_\sigma(6) &= \{4,6\} \\ \mathsf{Orb}_\sigma(3) &= \{3\} \end{aligned}$$

□

Problem 7.6 (Problem 7 Fraleigh's p.94). *Compute:*

$$(1\ 4\ 5)(7\ 8)(2\ 5\ 7)$$

Solution.

$$\begin{aligned} (1\ 4\ 5)(7\ 8)(2\ 5\ 7) &= (1\ 4\ 5) \circ ((7\ 8)(2\ 5\ 7)) \\ &= (1\ 4\ 5)(2\ 5\ 8\ 7) \\ &= (2\ 1\ 4\ 5\ 8\ 7) \end{aligned}$$

□

Problem 7.7 (Problem 29 Fraleigh's p.96). *Show that for every subgroup H of S_n for $n \geq 2$, either all permutations in H are even or exactly half are.*

Proof. Recall that an even permutation is a permutation which can be expressed as an even number of transpositions (swaps of 2 elements).

Let $\mathsf{sgn}(\sigma) = 1$ if σ is even, $\mathsf{sgn}(\sigma) = -1$ otherwise for all $\sigma \in S_n$. $\mathsf{sgn} : S_n \to \{1, -1\}$ is a homomorphism. Restrict this map to H. Then, the image:

$$\mathsf{sgn}[H] = \begin{cases} \{+1\} \\ \{+1, -1\} \end{cases}$$

In the first case it is clear that every element of H must be even.

In the other case where sgn is surjective, the kernel

$$\ker(\mathsf{sgn}[H]) = H \cap A_n,$$

the set of even permutations in H. By the first isomorphism theorem,

$$H/(H \cap A_n) \cong \{+1, -1\}$$

so

$$[H : H \cap A_n] = 2$$

hence

$$|H \cap A_n| = \frac{1}{2}H$$

i.e. half of H is even. $\square$

8 External- and Internal Direct Products

Definition 8.1. *Let* $H, K \leq G$,

$$G' = H \times K = \{(h,k) \mid h \in H,\ \ k \in K\}$$
$$G = H \oplus K = \{hk \mid h \in H,\ \ k \in K\}$$

The internal direct product $H \oplus K$ *presupposes that* $H, K \trianglelefteq G$, *and* $H \cap K = \{e\}$.

We really want to be able to say that $H \times K \cong H \oplus K$.

Example 8.1. *Consider the dihedral group* $D_3 = \{1, x, x^2, y, xy, x^y\}$. *Let* $H = \langle x \rangle$ *and* $K = \langle y \rangle$. *It's easy to see that* $H \cap K = \{e\} = \{1\}$, *and* $H \trianglelefteq D_3$. *However* $xK = \{x, xy\}$, *but* $Kx = \{x, yx\} = \{x, x^2y\}$. *Hence*

$$D_3 \neq H \oplus K$$

Lemma 8.1. $H, K \trianglelefteq G$ *and* $H \cap K = \{e\}$.

1. *if* $ab = a'b'$ *where* $a, a' \in H$ *and* $b, b' \in K$ *then* $a = a'$ *and* $b = b'$.
2. *if* $a \in H$ *and* $b \in K$ *then* $ab = ba$.

Theorem 8.1. *Assuming* H, K *normal subgroups of* G *with trivial intersection, then*

$$H \times K \cong H \oplus K$$

Proof. Define a map

$$\varphi : H \times K \to HK, \qquad \varphi(h,k) = hk.$$

This map is well-defined since $h \in H$, $k \in K$ implies $hk \in HK$.

Define a second map

$$\psi : HK \to H \times K$$

by sending $g \in HK$ to the unique pair (h,k) such that $g = hk$. Such a decomposition exists since $HK = G$, and is unique because $H \cap K = \{e\}$.

We now verify that these maps are inverse to one another. For all $(h,k) \in H \times K$,

$$(\psi \circ \varphi)(h,k) = \psi(hk) = (h,k),$$

and for all $g \in HK$,

$$(\varphi \circ \psi)(g) = g.$$

Thus φ is bijective with inverse ψ.

Finally, φ is a homomorphism, since for $(h_1, k_1), (h_2, k_2) \in H \times K$,

$$\begin{aligned}\varphi((h_1, k_1)(h_2, k_2)) &= \varphi(h_1 h_2, k_1 k_2) \\ &= h_1 h_2 k_1 k_2 \\ &= h_1 k_1 h_2 k_2 \\ &= \varphi(h_1, k_1)\varphi(h_2, k_2),\end{aligned}$$

where we use that elements of H and K commute.

Therefore φ is an isomorphism, and $HK \cong H \times K$. □

Theorem 8.2. *If $|x|, |y| < \infty$ and $(x, y) \in G \times H$ then $|(x, y)| = \mathrm{lcm}(|x|, |y|)$.*

9 Problems from week of 8 Feb

Problem 9.1 (Problem 47 Fraleigh's p.113). *Let G be an abelian group. Let $H \subseteq G$ consisting of the identity and all elements of H with order 2. Show that $H \leq G$.*

Proof. Let $H = \{e\} \cup \{g \in G \mid |g| = 2\} \subseteq G$. Let $x, y \in H$, and for the sake of simplicity assume they are nontrivial, i.e. $x \neq e \neq y$. To show that H constitutes a subgroup of G it suffices to show that $xy^{-1} \in H$ (we already know it is nonempty).

$$\begin{aligned}(xy^{-1})^2 &= xy^{-1}xy^{-1} \\ &= xxy^{-1}y^{-1} && (G \text{ abelian}) \\ &= x^2(y^2)^{-1} \\ &= e(e) \\ &= e\end{aligned}$$

Hence $|xy^{-1}| = 2$, so $xy^{-1} \in H$. Thus H is a subgroup of G. □

Problem 9.2 (Problem 52 Fraleigh's p.113). *Show that a finie abelian group is not cyclic if and only if it contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p.*

Proof. Let G be a finite abelian group.

We begin by proving the right-to-left implication. Assume then that there is some $H \leq G$ with $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Suppose, for a contradiction, that $G = \langle g \rangle$ (cyclic) for some $g \in G$. Let $\phi : H \to \mathbb{Z}_p \times \mathbb{Z}_p$ be an isomorphism.

Recall that as G is cyclic, generated by g, we have that there is some $k \in \mathbb{Z}$, for every $h \in H$, such that $h = k \cdot g$. As G is finite, $k \cdot g = (|G| - k) \cdot g$, so we can safely assume $k \geq 0$ without any loss of generality.

Since ϕ is bijective we know that, for every $y \in \mathbb{Z}_p \times \mathbb{Z}_p$, there is some $h \in H$ such that

$$\phi(h) = y$$

Using the homomorphism property, and the fact that $h = kg,\ k \in \mathbb{N}$, we

get that:

$$\begin{aligned} y &= \phi(h) \\ &= \phi(k \cdot g) \\ &= \phi\left(\sum_{i=1}^{k} g\right) \\ &= \sum_{i=1}^{k} \phi(g) \\ &= k \cdot \phi(g) \end{aligned}$$

As y was chosen arbitrarily we now see that $\mathbb{Z}_p \times \mathbb{Z}_p = \langle \phi(g) \rangle$, i.e. cyclic. Being cyclic, together with the fact that $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2$, it is the case that there must be some element with order p^2, but no such element exists so $\mathbb{Z}_p \times \mathbb{Z}_p$ is not cyclic. We have arrived at a contradiction so our assumption that G is cyclic must be false.

Now we prove the other direction. We now assume that we have a finite abelian group G which is not cyclic. As G is finite we know that G is finitely generated. Thus by the fundamental theorem of finitely generated abelian groups we know that G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{(p_1)^{\gamma_1}} \times \mathbb{Z}_{(p_2)^{\gamma_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{\gamma_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

As G is finite, the direct product does not include $\mathbb{Z}$. Furthermore as G is not cyclic we know that

$$G \ncong \mathbb{Z}_{p^\gamma}$$

Hence G must be the direct product of at least 2 $\mathbb{Z}_{(p_i)^{\gamma_i}}$. As $\gamma_i \in \mathbb{N} \setminus \{0\}$ and distinct from γ_j for $j \neq i$ there must be some $\mathbb{Z}_{(p_i)^{\gamma_l}}$ with $\gamma_l \geq 2$. Notice that this group necessarily has

$$H = \{0\} \times \cdots \times \{0\} \times \mathbb{Z}_{p_i} \times \{0\} \times \cdots \times \{0\} \times \mathbb{Z}_{p_i} \times \{0\} \times \cdots \times \{0\}$$

as a subgroup, which itself is isomorphic to $\mathbb{Z}_{p_i} \times \mathbb{Z}_{p_i}$. Then $\phi^{-1}[H]$ is a subgroup of G, which is isomorphic to $\mathbb{Z}_{p_i} \times \mathbb{Z}_{p_i}$. □

Problem 9.3 (Problem 46 Fraleigh's p.135). *Let a group G be generated by $\{a_i \mid i \in I\}$, where I is some indexing set and $a_i \in G$ for all $i \in I$. Let ϕ, μ be two homomorphisms from G into a group G', such that $\phi(a_i) = \mu(a_i)$ for every $i \in I$. Prove that $\phi = \mu$.*

Proof. Let $G = \{a_i \mid i \in I\}$ with homomorphisms $\phi, \mu : G \to G'$ which

coincide on a_i for all $i \in I$. Let $x \in G$.

$$\begin{aligned}
\phi(x) &= \phi\left(\prod_{i\in I} a_i^{k_i}\right),\ k_i \in \mathbb{Z} \\
&= \prod_{i\in I} \phi(a_i^{k_i}) \\
&= \prod_{i\in I} \underbrace{\phi(a_i)\cdots\phi(a_i)}_{k_i \text{ times}} \\
&= \prod_{i\in I} \underbrace{\mu(a_i)\cdots\mu(a_i)}_{k_i \text{ times}} \\
&= \prod_{i\in I} \mu(a_i^{k_i}) \\
&= \mu\left(\prod_{i\in I} a_i^{k_i}\right) = \mu(x)
\end{aligned}$$

x was chosen arbitrarily hence ϕ and μ coincide on all $x \in G$. In other words, $\phi = \mu$. □

Problem 9.4 (52 Fraleigh's p.135). *Let $\phi : G \to G'$ be a homomorphism with kernel H and let $a \in G$. Prove the set equality $\{x \in G \mid \phi(x) = \phi(a)\} = Ha$.*

Proof. We begin by proving that $Ha \subseteq \{x \in G \mid \phi(x) = \phi(a)\}$.

Suppose $ha \in Ha$. Then $h \in H$ so

$$\phi(ha) = \underbrace{\phi(h)}_{\in H}\phi(a) = e'\phi(a) = \phi(a)$$

Thus $ha \in \{x \in G \mid \phi(x) = \phi(a)\}$. As x was arbitrarily chosen, we conclude that

$$Ha \subseteq \{x \in G \mid \phi(x) = \phi(a)\}$$

Let $x \in \{x \in G \mid \phi(x) = \phi(a)\}$. Then

$$\begin{aligned}
\phi(x) &= \phi(a) \\
\phi(x)\phi(a)^{-1} &= e' \\
\phi(xa^{-1}) &= e'
\end{aligned}$$

hence $xa^{-1} \in H$ which implies $x \in Ha$. Once again x was arbitrarily chosen so

$$\{x \in G \mid \phi(x) = \phi(a)\} \subseteq Ha$$

Summing up we conclude that

$$Ha = \{x \in G \mid \phi(x) = \phi(a)\}$$

□

10 Problems week of 16 Feb, Quotient grps, simple grps

Problem 10.1 (Problem 3 Fraleigh's p.142). *Find the order of the given factor group:*

$$(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(2,1)\rangle$$

Solution. We first compute the subgroup generated by $(2,1)$:

$$\langle(2,1)\rangle = \{(0,0),(2,1)\},$$

since $(2,1)+(2,1)=(0,0)$.

Because $\mathbb{Z}_4 \times \mathbb{Z}_2$ is abelian, every subgroup is normal, so the quotient group is well-defined.

The elements of the quotient

$$(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(2,1)\rangle$$

are the cosets

$$(x,y)+\langle(2,1)\rangle = \{(x,y),(x+2,y+1)\}, \quad (x,y) \in \mathbb{Z}_4 \times \mathbb{Z}_2.$$

Each coset has exactly 2 elements. Since

$$|\mathbb{Z}_4 \times \mathbb{Z}_2| = 8,$$

the number of distinct cosets is

$$\frac{8}{2} = 4.$$

Hence the quotient group has order 4. □

Problem 10.2 (Problem 34 Fraleigh's p.143). *Show that if a finite group G has exactly one subgroup H of a given order, then H is a normal subgroup of G.*

Proof. Suppose G is a finite group with only one subgroup H of some order $k \in \mathbb{N}$. Recall that for the conjugacy of H is still a subgroup, furthermore

$$|gHg^{-1}| = |H| = k,\ g \in G$$

However H is the only subgroup with order k so

$$gHg^{-1} = H,\ \forall g \in G$$

which implies that H is normal.

□

Problem 10.3 (Problem 35 Fraleigh's p.143). *Show that if H and N are subgroups of a group G, and N is normal in G, then $H \cap N$ is normal in H.*

Proof. Let G be a group with $H \leq G$ and $N \trianglelefteq G$. We take it for granted that $H \cap N$ is indeed a group (this is not hard to show).

Fix some arbitrary $h \in H$. We must show that $h(H \cap N)h^{-1} \subseteq H \cap N$.

Let $x \in H \cap N$. As $x, h \in H$ we ceirtanly have $hxh^{-1} \in H$. As $x \in N$, N normal, we have that for any $h \in H \subseteq G$, $hxh^{-1} \in N$.

Hence

$$hxh^{-1} \in H \cap N$$

□

Problem 10.4 (Problem 3 Fraleigh's p.151). *Classify the groups according to the fundamental theorem of finitely generated abelian groups.*

$$(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1,2)\rangle$$
$$(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$$
$$(\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2,4)\rangle$$

Solution. We begin with $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1,2)\rangle$.

$$\begin{aligned}
\langle(1,2)\rangle &= \{(0,0),(1,2)\} \\
(0,0)\{(0,0),(1,2)\} &= \{(0,0),(1,2)\} = A \\
(1,0)\{(0,0),(1,2)\} &= \{(1,0),(0,2)\} = B \\
(0,1)\{(0,0),(1,2)\} &= \{(0,1),(1,3)\} = C \\
(1,1)\{(0,0),(1,2)\} &= \{(1,1),(0,3)\} = D \\
(0,2)\{(0,0),(1,2)\} &= \{(1,0),(0,2)\} = B \\
(1,2)\{(0,0),(1,2)\} &= \{(1,2),(0,0)\} = A \\
(0,3)\{(0,0),(1,2)\} &= \{(0,3),(1,1)\} = D \\
(1,3)\{(0,0),(1,2)\} &= \{(1,3),(0,1)\} = C
\end{aligned}$$

We get an abelian group with 4 distinct elements. Crucially, we can see that the coset of $(0,1)$ has order 4 and is thus a generator. We conclude that $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1,2)\rangle \cong \mathbb{Z}_4$.

Now we look at $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$.

Notice that

$$(\mathbb{Z}_4 \times \mathbb{Z}_8) = \langle a, b \mid 4a = 0,\ 8b = 0,\ ab = ba\rangle$$

so quotienting with $\langle(1,2)\rangle$ only imposes the extra relation that

$$a + 2b = 0 \Leftrightarrow a = -2b$$

then $\text{ord}(1,2) = \text{lcm}(4,4) = 4$ so $\langle(1,2)\rangle$ has 4 elements. $|\mathbb{Z}_4 \times \mathbb{Z}_8| = 32$ so the quotient group has

$$\frac{32}{4} = 8$$

elements. Up to isomorphism there exist 3 abelian groups of order 8. The relation imposed by $\langle(1,2)\rangle$ changes nothing so we require $8b = 0$. Clearly

$$(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle \cong \mathbb{Z}_8$$

Lastly we look at

$$(\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2,4)\rangle$$

Notice that

$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8 = \{a, b, c \mid 4a = 0,\ 4b = 0,\ 8c = 0,\ ab = ba,\ ac = ca,\ bc = ca\}$$

with

$$\langle(1,2,4)\rangle$$

imposing $a + 2b + 4c = 0$ which then means that $a = -2b - 4c$. The order of $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8$ is 128. The order of the subgroup is $\text{lcm}(4,2,2)$ which is 4. Thus the order of the quotient group is

$$\frac{128}{4} = 32 = 2^5$$

There are precisely 7 abelian groups unique up to isomorphism. b has order 4 and c has 8 so we conclude that the quotient group is isomorphic to

$$\mathbb{Z}_4 \times \mathbb{Z}_8$$

□

Problem 10.5 (Problem 34 Fraleigh's p.153). *Let G be finite, containing a nontrivial subgroup of index 2 in G. Show that G is not simple.*

Proof. There exists a subgroup $H \leq G$ with 2 left cosets. Since H is always a left coset of H there must be one more left coset gH for any $g \notin H$. Since the number of right cosets is the same we have right cosets H and Hg. There are only 2 cosets so the non-H cosets must be the same

$$gH = Hg$$

Thus left and right cosets coincide. Therefore

$$H \trianglelefteq G$$

H is nontrivial, and crucially $H \neq G$ (since the index is 2). Hence G has a nontrivial proper subgroup. In other words, G is not simple. □

11 Group Actions

Definition 11.1. *Let X be a set, and G a group. A (left) action of G on X is a map*

$$G \times X \to X$$
$$(g, x) \mapsto gx$$

such that $ex = x$ and $g_1(g_2 x) = (g_1 g_2)x$ for all $x \in X$ and $g_1, g_2 \in G$.

The right action is similarily defined, and in the case where G is abelian the actions coincide.

Example 11.1. *The following constitute group actions when considering matrix-vector multiplication.*

1. *$GL_2(\mathbb{R})$ and its subgroups on $\mathbb{R}^2$.*
2. *same for $GL_n(\mathbb{R})$ on $\mathbb{R}^n$.*

A very natural group action is D_n acting on the regular polygon with n sides, as D_n is the symmetries of the regular n-gon. Furthermore S_n (which is often thought of as the bijections $f : [n] \to [n]$) can act on said $[n]$.
Another group action which we have also seen many times is conjugation where G acts on itself.

Definition 11.2. *Let G be a group and X a set.*
We say that a group action $G \times X \to X$ is faithful *if for any $g \in G$, $g \neq e$ implies there is some $x \in X$ such that $gx \neq x$.*
Alternatively it can be defined to be a group action for which any $g_1, g_2 \in G$ with $g_1 \neq g_2$ implies that there exists $x \in X$ such that $g_1 x \neq g_2 x$.

Proposition 11.1. *Consider a group action $G \times X \to X$. It defines a group homomorphism $\phi : G \to \mathrm{Sym}(X)$ for which $\ker \phi = \{e\}$ if and only if the group action is faithful.*

Problem 11.1 (Problem 11 Fraleigh's p.160). *Let X be a G-set. Show that G acts faithfully on X if and only if no two distinct elements of G have the same action on each element X.*
(I.e. prove the equivalent definition posed in definition 11.2)

Proof. Let G be a group, X a G-set.

Assume first that the action of G on X is faithful. Then $e \neq g \in G$ implies the existence of some $x \in X$ for which

$$gx \neq x$$

Suppose, for a contradiction, that there exist some distinct $g_1, g_2 \in G$ which coincide on every $x \in X$. Then

$$g_1 x = g_2 x$$
$$g_2^{-1} g_1 x = x$$

In other words there exists $g = g_2^{-1} g_1 \in G$ for which every $x \in X$ is a fixed-point, contradicting the assumption that G acts faithfully on X. Thus G acting faithfully on X must imply that any distinct pair of elements of G have some $x \in X$ for which they do not coincide.

Assume now that G acts on X such that for every distinct $g_1, g_2 \in G$ for which there exists $x \in X$ such that $g_1 x \neq g_2 x$. Let $g_2 = e \neq g_1$. They are clearly distinct and furthermore

$$g_1 x \neq g_2 x = x$$

This holds for any $g_1 \in G$ so G acts faithfully on X. □

Definition 11.3 (Orbit). *Let G be a group acting on a G-set X. Let $x \in X$.*
The orbit of x, often denoted $\mathit{Orb}(x)$ or Gx is the set

$$\mathit{Orb}(x) := \{gx \mid g \in G\}$$

Definition 11.4 (Stabilizer). *Let G be a group acting on a G-set X. Let $x \in X$.*
The stabilizer of x, often denoted $\mathit{Stab}_G(x)$ or G_x is the set

$$\{g \in G \mid gx = x\}$$

Theorem 11.1 (Orbit-Stabilizer). *For a finite group G acting on a set X, the following holds (conditions are equivalent).*

$$|\mathit{Orb}(x)| = [G : \mathit{Stab}_G(x)]$$
$$|G| = |\mathit{Orb}(x)| \cdot |\mathit{Stab}_G(x)|$$

Problem 11.2. *Let $\{X_i \mid i \in I\}$ be a disjoint collection of sets. Let each X_i be a G-set for the same group G.*
*a) Show that $\bigcup_{i\in I} X_i$ can be viewed in a natural way as a G-set, the **union** of the G-sets X_i.*
b) Show that every G-set X is the union of its orbits.

Proof of (a). Let $X = \bigcup_{i\in I} X_i$. Since the union is disjoint, each $x \in X$ lies in a unique X_i. Define

$$g \cdot x := g \cdot_{X_i} x$$

where the right-hand side denotes the given G-action on X_i.

This is well-defined because the union is disjoint. For $x \in X_i$ we have

$$e \cdot x = x$$

since X_i is a G-set, and

$$(gh) \cdot x = (gh) \cdot_{X_i} x = g \cdot_{X_i} (h \cdot_{X_i} x) = g \cdot (h \cdot x).$$

Thus the action axioms hold, and X becomes a G-set. □

Proof of (b). For $x \in X$, define the orbit

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

Since $x = e \cdot x$, every element lies in its orbit, so

$$X = \bigcup_{x\in X} G \cdot x.$$

If $G \cdot x \cap G \cdot y \neq \emptyset$, then $g \cdot x = h \cdot y$ for some $g, h \in G$. Then

$$x = g^{-1}h \cdot y,$$

so $x \in G \cdot y$, which implies $G \cdot x = G \cdot y$. Thus distinct orbits are disjoint, and X is the disjoint union of its orbits. □

Theorem 11.2 (Burnside's Formula). *Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G, then*

$$r \cdot |G| = \sum_{g \in G} |X_g|$$

where X_g are the fixed points *of g, namely all $x \in X$ satisfying $gx = x$.*

Problem 11.3 (Problem 1 Fraileigh's p.164). *Find the number of orbits in $\{1, \dots, 8\}$ under the cyclic subgroup $\langle (1\ 3\ 5\ 6) \rangle \leq S_8$.*

Solution. Both $[8]$ and the given subgroup of S_8 are finite so we use Burnside's formula. Denote $\langle \sigma \rangle := \langle 1\ 3\ 5\ 6 \rangle$. We know that $|\sigma| = 4$ so we must simply calculate the sum of sizes of fixed points of each permutation in $\langle \sigma \rangle$. Obviously $|X_e| = |X| = 8$. Next up σ has $2, 4, 7, 8$ as fixed points so $|X_\sigma| = 4$. Next up $\sigma^2 = (1\ 5)(3\ 6)$ and has the same fixed points. $\sigma^3 = (1\ 6\ 5\ 3)$ with the same fixed points once again. Thus

$$r = 8 + 4 + 4 + 4/|\sigma| = 5$$

□

12 Rings, Fields & Integral domains

Definition 12.1 (Ring). *A ring R is a set together with two binary operations $+$ and $\cdot$, written $(R, +, \cdot)$, satisfying*

1. *$(R, +)$ is an abelian group (identity denoted 0),*
2. *$(R, \cdot)$ has closure and associativity,*
3. *with distributive laws, i.e.*

$$a \cdot (b + c) = ab + ac, \quad (b + c) \cdot a = ba + ca.$$

If R has a multiplicative identity 1, we say R is a ring with identity, or R is a ring with unity or R is unital.
If $ab = ba$ for all $a, b \in R$, then R is a commutative ring.

So what, informally, a ring is, is a structure where you can add, multiply and subtract, but not necessarily divide.

Rings have a bunch of immediately nice properties such as

- $0 \in R$ is unique (follows from $(R, +)$ being abelian grp),
- $-a$ is unique (follows from the same logic),
- $a \cdot 0 = 0 = 0 \cdot a$ (very nice),
- $|R| \geq 2$, then $1 \neq 0$,
- $-(a + b) = (-a) + (-b)$,
- $-(-a) = a$,
- $-(ab) = (-a)b = a(-b)$,
- $ab = (-a)(-b)$.

Definition 12.2 (Unit). *Let $(R, +, \cdot)$ be a ring with identity, and let $u \in R$. u is called a unit if u has a multiplicative inverse u^{-1} such that*

$$u \cdot u^{-1} = u^{-1} \cdot u = 1$$

We denote the set of units

$$\{u \in R \mid u \text{ unit}\} =: R^x$$

(This set is a group under the multiplication of R)

Definition 12.3 (Zero divisor). *Let $(R, +, \cdot)$ be a ring. A zero divisor is a non-zero element $a \in R$ such that there exists non-zero $b \in R$ satisfying*

$$ab = 0 \quad \text{left zero divisor} \qquad ba = 0 \quad \text{right zero divisor}$$

Where these coincide in commutative rings.

Definition 12.4 (Field). *Let $(R, +, \cdot)$ be a ring.*
*R is a **field** if $(R \setminus \{0\}, \cdot)$ is an abelian group.*

Definition 12.5. *Let $(R, +, \cdot)$ be a ring.*
*R is a **division ring** if $(R \setminus \{0\}, \cdot)$ is a group.*

Crucially, in both a divison ring and a field we know that $\exists 1 \in R$, the multiplicative identity, meaning a field/division ring is unital.

The prototypical example of a commutative unital ring is $(\mathbb{Z}, +, \cdot)$. Importantly, $\mathbb{Z}$ is not a field. So a big area of focus will be to look at larger more powerful structures.

Definition 12.6 (Integral Domain). *Let $(R, +, \cdot)$ be a ring.*
*R is an **integral domain** if it is a commutative, unital ring.*

Proposition 12.1. *A ring R is an integral domain if and only if R has no zero-divisors and $|R| \geq 2$.*

The nice property we can gleam from integral domains is that $a \cdot b = 0$ if and only if either a or b is zero.

Usually, when we say integral domain, or field, we will be refering to said structure when it has 2 or more elements. The reason for this is that a ring or field with 1 element is not worth dwelling on.

Proposition 12.2. *A field is an integral domain.*

Proof sketch. If $ab = 0$ and $a \neq 0$, then $b = a^{-1}(ab) = a^{-1}0 = 0$. □

Theorem 12.1. *Every finite integral domain is a field.*

Proof. Let D be a finite integral domain.

$(D \setminus \{0\}, \cdot)$ is closed, because D has no zero divisors. Furthermore it

is associative and $1 \in D \setminus \{0\}$ by definition. The last thing we need is inverses.

Let $r \in D$, $r \neq 0$. Consider $r, r^2, r^3, \ldots r^k, \ldots$

As D is finite there must be repeted powers in this list. Let $r^i = r^j$, $i < j$ wlog. Then

$$\underbrace{r \cdot r \cdots r}_{i} \cdot 1 = \underbrace{r \cdot r \cdots r}_{j}$$

Use left cancellation repeatedly to get

$$r^{j-i} = 1$$

Let $s = r^{j-i-1}$. Then $rs = sr = 1$, so $s = r^{-1}$. □

Theorem 12.2. *Every finite division ring is a field.*

13 Some problems pertaining to Rings, Fields, etc.

Problem 13.1 (Problem 3 & 5 Fraleigh's p.174). *Compute the products*

$$(11)(-4) \in \mathbb{Z}_{15}$$

$$(2,3)(3,5) \in \mathbb{Z}_5 \times \mathbb{Z}_9$$

Solution.

$$\begin{aligned} 11 \cdot -4 &= -(11 \cdot 4) \\ &= -(44) \\ &\equiv 1 \mod 15 \end{aligned}$$

$$\begin{aligned} (2,3)(3,5) &= (2 \cdot 3, 3 \cdot 5) \\ &= (6,15) \\ &\equiv (1,6) \end{aligned}$$

□

Problem 13.2 (Problem 11 Fraleigh's p.175). *Determine whether the following structure is a ring, then if it is a commutative ring, whether it is unital, and whether it is a field.*

$$\left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \right\}$$

Solution. Let's denote this structure as $\mathbb{Z}(\sqrt{2})$.

It is quite clear that $(\mathbb{Z}(\sqrt{2}), +)$ forms an abelian group as the integers is an abelian group and the identity here is $0 + 0\sqrt{2} \in \mathbb{Z}(\sqrt{2})$. Furthermore $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Z}(\sqrt{2})$, so we're good.

The $\mathbb{Z} \setminus \{0\}$ with multiplication is closed, but not every element has an inverse (in fact only 1 and -1 do), so we'd expect something similar here.

Suppose $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Z}(\sqrt{2}) \setminus \{0\}$. Then

$$\begin{aligned} (a + b\sqrt{2})(c + d\sqrt{2}) &= ac + cb\sqrt{2} + ad\sqrt{2} + 2bd \\ &= (ac + 2bd) + (ad + cb)\sqrt{2} \in \mathbb{Z}(\sqrt{2}) \setminus \{0\} \end{aligned}$$

So the multiplicative structure is closed with identity, but there does not exist inverses for every element as for instance $2 \in \mathbb{Z}(\sqrt{2})^x$, but

2^{-1} does not exist. It is also not hard to see that distributive laws work fine.

Thus we conclude that $\mathbb{Z}(\sqrt{2})$ is a commutative unital ring. □

Problem 13.3 (Problem 20 Fraleigh's p.175). *Consider the matrix ring $M_2(\mathbb{Z}_2)$.*
a. Find the order (number of elements) of the ring.
b. List all units in the ring.

Solution of (a). Recall that

$$M_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{Z}_2 \right\}$$

There are 4 entries in each matrix in the ring, all of which can take on one of two values from $\mathbb{Z}_4$. Thus there are $2^4 = 16$ elements. □

Problem 13.4 (Problem 37 Fraleigh's p.176). *Show that if U is the collection of all units in a ring $(R, +, \cdot)$ with unity, then $(U, \cdot)$ is a group.*

Proof. We conisder U the collection of the units of a ring R. $1 \in R$ (as R has unity), $(R, \cdot)$ has associativity by definition and the set of units U is precisely those $u \in R$ such that

$$u \cdot u^{-1} = u^{-1} \cdot u = 1$$

so it remains to show that U is closed. Let $u, v \in U$. Then, as said, there exists inverses $u^{-1}, v^{-1} \in U$. Then

$$\begin{aligned} (uv)(v^{-1}u^{-1}) &= u(vv^{-1})u^{-1} \\ &= u(1)u^{-1} \\ &= uu^{-1} \\ &= 1 \end{aligned}$$

so $(uv)^{-1} = (v^{-1}u^{-1}) \in U$. Thus the product of two units is itself a unit. We have shown $(U, \cdot)$ to have all the properties of a group. □

Problem 13.5 (Problem 46 Fraleigh's p.176). *An element a of a ring R is nilpotent if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Show that if a and b are nilpotent in some ring commutative ring R, then $a + b \in R$ is also nilpotent.*

Proof. Suppose $a, b \in R$ (commutative) such that $a^n = 0$ and $b^m = 0$ for some $n, m \in \mathbb{Z}^+$.

Let $k \in \mathbb{Z}^+$. Then

$$\begin{aligned}(a+b)^k &= \sum_{i=0}^{k} \binom{k}{i} a^{k-i} b^i \\ &= a^k + ka^{k-1}b + \cdots + kab^{k-1} + b^k\end{aligned}$$

in particular, if $k := n + m$ then we observe the following:

$$\begin{aligned}(a+b)^{n+m} &= \sum_{k=0}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k \\ &= \sum_{k=m+1}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k + \sum_{k=0}^{m} \binom{n+m}{k} a^{n+m-k} b^k \\ &= \underbrace{\binom{n+m}{m+1} a^{n+m-m-1} b^{m+1}}_{\cdots\, a^{n-1} \cdot 0 \cdot b = 0} + \ldots + \underbrace{b^{n+m}}_{(b^n)\cdot 0 = 0} \\ &\quad + \underbrace{a^{n+m}}_{0 \cdot a^m = 0} + \cdots + \underbrace{\binom{n+m}{m} a^{n+m-m} b^m}_{\cdots\, 0 \cdot 0 = 0} \\ &= 0\end{aligned}$$

since every term is 0. □

Problem 13.6 (Problem 1 Fraleigh's p.182). *Find all solutions of* $x^3 - 2x^2 - 3x = 0$ *in* $\mathbb{Z}_{12}$.

Solution.

$$\begin{aligned}f(x) = x^3 - 2x^2 - 3x &= 0 \\ x(x^2 - 2x - 3) &= 0 \\ x(x-3)(x+1) &= 0\end{aligned}$$

Since we are in a ring with zero-divisors we are really asking for which $x \in \mathbb{Z}_{12}$ the following holds

$$12 \mid x(x-3)(x+1)$$

We begin by solving $\mod 3$ where

$$f(x) = x^2(x+1) \in \mathbb{Z}_3[x]$$

with solutions $0, 2 \in \mathbb{Z}_3$. $f(x)$ reduces to

$$f(x) = x(x-1)^2 \in \mathbb{Z}_4[x]$$

with solutions $0, 1, 2 \in \mathbb{Z}_4$. We get the solutions

$$\{0, 2, 5, 6, 8, 9\} \subset \mathbb{Z}_{12}$$

□

Problem 13.7 (Problem 11 Fraleigh's p.182). *Let R be a commutative unital ring with characteristic 4. Compute and simplify $(a+b)^4$ for $a, b \in R$.*

Solution.

$$\begin{aligned}(a+b)^4 &= a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + b^4 \\ &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4\end{aligned}$$

As $4 \equiv 0 \mod 4$ and $6 \equiv 2 \mod 4$ we get $(a+b)^4 \equiv a^4 + 2a^2b^2 + b^4$ in integral domain R with $\text{char}(R) = 4$. □

Problem 13.8 (Problem 23 Fraleigh's p.183). *Show that a division ring has exactly two idempotent elements.*

Proof. Recall that we define division rings as non-trivial so $|R| \geq 2$ crucially. The candidates for idempotent elements are $0, 1 \in R$ as $0 \cdot 0 = 0$ as $0 \cdot a = 0 \; \forall a \in R$. Then since $1 \cdot a = a \; \forall a \in R$ we conclude that $1 \cdot 1 = 1$. Now we need to show that there do not exist any other elements which satisfy this property. Assume, for a contradiction, that there exists $a \in R \setminus \{0, 1\}$ such that

$$a^2 = a$$

As R is a division ring we know there exists $a^{-1} \in R$ such that

$$\begin{aligned}a^2a^{-1} &= aa^{-1} \\ a(aa^{-1}) &= 1 \\ a &= 1\end{aligned}$$

contradiction our assumption that $a \neq 1$. □

Problem 13.9 (Problem 29 Fraleigh's p.183). *Show that the characteristic of an integral domain D is either 0 or a prime p.*

Proof. Let D be an integral domain, i.e. a commutative ring with unity and no zero-divisors. Assume, for a contradiction, that $\text{char}(D) = k \in$

$\mathbb{Z}^+$ (not prime). Then $\text{char}(D) = k = nm,\ n, m \in \mathbb{Z}^+$. Then we can conclude that

$$k \cdot 1 = \underbrace{1 + 1 + \cdots + 1 + 1}_{k=nm \text{ times}} = 0$$

but then

$$(n \cdot 1)(m \cdot 1) = 0$$

so $n \cdot 1 = 0$ or $m \cdot 1 = 0$ so k is not the characteristic of D. $\square$

14 Fermat's and Euler's theorems, Quotient Fields

Theorem 14.1 (Fermat's Little Theorem). *If p is prime and* $\gcd(a,p) = 1$, *then*

$$a^{p-1} \equiv 1 \mod p$$

Equivalently

$$a^p \equiv a \mod p$$

Proof idea. The key fact is that

$$(\mathbb{Z}/p\mathbb{Z})^\times$$

the nonzero elements mod p, form a group under multiplication. This group has $p-1$ elements (finite) and cyclic. By Lagrange's Theorem, if G is finite and $g \in G$ then

$$g^{|G|} = e$$

Applying this to $G = (\mathbb{Z}/p\mathbb{Z})^\times$ we get

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

□

Theorem 14.2. *Euler's Theorem If* $\gcd(a,n) = 1$, *then*

$$a^{\phi(n)} \equiv 1 \mod n,$$

where $\phi(n)$ is Euler's totient function.

Proof idea. We consider

$$(\mathbb{Z}/n\mathbb{Z})^\times$$

the group of units mod n. It has exactly $\phi(n)$ elements. Again by Lagrange:

$$a^{\phi(n)} \equiv 1$$

□

So Fermat's Little Theorem is just Euler's Theorem for n prime.

14.1 Quotient Fields

In $\mathbb{Z}$, you generally cannot divide by 2. But in $\mathbb{Q}$, you can. The questions we want to answer is:

"Can we build a field from a ring?"

As it turns out the answer is yes (conditions may apply...).

Recall that an integral domain is

- a commutative ring,
- with identity,
- with no zero divisors

Suppose D is an integral domain. We construct $\text{Frac}(D)$ like rational numbers.

Definition 14.1 (Quotient Field). *The **field of fractions** or **quotient field** of an integral domain D is the smallest field K (often denoted $\text{Frac}(D)$) containing D as a subring, constructed by forming formal fractions $\frac{a}{b}$ where $a, b \in K$ $(b \neq 0)$.*
The operations on K are defined as

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bd}{bd}$$

and

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

We equip K with an equivalence relation $\sim$ where we say

$$\frac{a}{b} \sim \frac{c}{d}$$

if $ad = bc$.

As we see we get a field $\text{Frac}(D)$ and we get an injective embedding

$$D \hookrightarrow \text{Frac}(D)$$

via

$$a \mapsto \frac{a}{1}$$

Problem 14.1 (Problem 20.5 Fraleigh's p.189). *Use Fermat's theorem to find the remainder of 37^{49} when it is divided by 7.*

Solution. $\gcd(37, 7) = 1$ and $p = 7$ is ceirtainly prime so Fermat's Little Theorem applies.

We can rewrite

$$37^{49} = 37^{7^2} \equiv 2^{7^2}$$

From FLT we have $2^6 \equiv 1$.

$$2^{7^2} = 2^{6 \cdot 8 + 1} \equiv 1^8 \cdot 2 \equiv 2 \mod 7$$

□

Problem 14.2 (Problem 20.12 Fraleigh's p.189). *Describe all solutions to*

$$22x \equiv 5 \mod 15$$

Solution. The greatest common divisor $\gcd(22, 15) = 1$ which is a divisor of 5 so there does exist solutions (in fact, as $\gcd(22, 15) = 1$ there exist exactly one solution). We can simplify to get

$$7x \equiv 5 \mod 15$$

As the greates common divisor is 1 we know that 7 is a unit in $\mathbb{Z}/15\mathbb{Z}$. We want to find 7^{-1}. Notice that $7 \cdot 13 = 91 \equiv 1$.

$$\begin{aligned} x &\equiv 13 \cdot 5 \mod 15 \\ 13 \cdot 5 &= 65 \\ 65 &\equiv 5 \mod 15 \end{aligned}$$

Thus

$$x \equiv 5 \mod 15$$

□

Problem 14.3 (Problem 20.15 Fraleigh's p.189). *As in the task above for*

$$39x \equiv 125 \mod 9$$

Solution. Notice that

$$39 \equiv 3 \mod 9$$

and

$$125 \equiv -1 \equiv 8 \mod 9$$

so we can transform the problem into

$$3x \equiv 8 \mod 9$$

Notice that $\gcd(3, 9) = 3$, but 3 is not a divisor of 8 thus the solution DNE. □

Problem 14.4 (Problem 20.27 Fraleigh's p.190). *Show that 1 and $p - 1$ are the only elements of the field $\mathbb{Z}_p$ that are their own multiplicative inverse. [Hint: Consider the equation $x^2 - 1 = 0$].*

Proof. Let p be prime and let $x \in \mathbb{Z}_p$. Notice that $x = x^{-1}$ iff

$$x^2 \equiv 1 \mod p \Leftrightarrow x^2 - 1 \equiv 0 \mod p$$

It is not hard to see that 1 and $p-1$ are solutions to these equations, but we have to show that they are the only ones. Notice that x^2-1 can be rewritten so we get

$$(x-1)(x+1) \equiv 0 \mod p$$

Recall that since $\mathbb{Z}_p$ is a field (no zero divisors) it is the case that $x-1 \equiv 0$ or $x+1 \equiv 0$. I.e.

$$x \equiv 1 \mod p, \ x \equiv -1 \mod p.$$

Therefore

$$x = \begin{cases} 1 \\ p-1 \end{cases}$$

□

Problem 14.5 (Problem 21.1 Fraleigh's p.196). *Describe the field F of quotients of the integral subdomain*

$$D = \{n + mi \mid n, m \in \mathbb{Z}\}$$

of $\mathbb{C}$. "Describe" means give the elements of $\mathbb{C}$ that make up the field of quotients of D in $\mathbb{C}$.

Solution. Recall that

$$\text{Frac}(D) = \left\{ \frac{a}{b} \,\middle|\, a, b \in D \ (b \neq 0) \right\}$$

$a, b \in D$ means that a, b can be written as

$$a = n + mi, \ b = k + li, \ n, m, k, l \in \mathbb{Z}$$

(note: $k + li \neq 0 \Rightarrow k \neq 0 \neq li$) so

$$\text{Frac}(D)$$

are elements of the form

$$\begin{aligned} \frac{n+mi}{k+li} &= \frac{n+mi}{k+li} \cdot \frac{k-li}{k-li} \\ &= \frac{(n+mi)(k-li)}{k^2+l^2} \\ &= \frac{nk + kmi - nli + ml}{k^2+l^2} \\ &= \frac{nk + ml + (km-nl)i}{k^2+l^2} \\ &= \frac{nk+ml}{k^2+l^2} + \frac{km-nl}{k^2+l^2} i \end{aligned}$$

Now we know $\mathsf{Frac}(D) \subseteq \mathbb{Q}(i)$, but is this subset relation strict? Let $a = r/s,\ b = t/s$. Then

$$a + bi = \frac{r}{s} + \frac{t}{s}i$$

and since

$$r + ti \in \mathbb{Z}(i) = D, \text{ and } s \in \mathbb{Z} \subset \mathbb{Z}(i) = D$$

we conclude that $\mathbb{Q}(i) \subseteq D$. I.e.

$$D = \mathsf{Frac}(\mathbb{Z}(i)) = \mathbb{Q}(i)$$

□