Lecture Notes

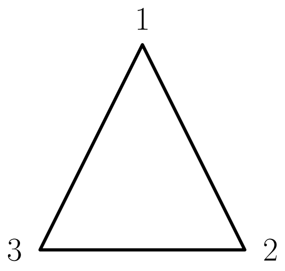
Cain Edie-Michell

Fall 2023

Contents

Lecture 1 (30-8-2023)

The goal of this lecture is to motivate the definition of a group. A group is an abstractification of the notion of symmetry. Hence we will use the symmetries of the equilateral triangle to motivate our definition



The symmetries of this triangle are

$$\begin{aligned} e &: \emptyset \\ r_{120} &: 1 \to 2 \to 3 \to 1 \\ r_{240} &: 1 \to 3 \to 2 \to 1 \\ f_1 &: 2 \leftrightarrow 3 \\ f_2 &: 1 \leftrightarrow 3 \\ f_3 &: 1 \leftrightarrow 2 \end{aligned}$$

We then have the set

$$G = \{e, r_{120}, r_{240}, f_1, f_2, f_3\}.$$

These symmetries have the additional structure that any two symmetries can be composed to give a new symmetry. For example if we do r_{120} then f_3, this is the same as doing the symmetry f_1. This composition can be described as a function

$$\circ : G \times G \to G.$$

It is convenient to express the function $\circ$ in table form as follows. This is typically called a Cayley table.

$\circ$	e	r_{120}	r_{240}	f_1	f_2	f_3
e	e	r_{120}	r_{240}	f_1	f_2	f_3
r_{120}	r_{120}	r_{240}	e	f_3	f_1	f_2
r_{240}	r_{240}	e	r_{120}	f_2	f_3	f_1
f_1	f_1	f_2	f_3	e	r_{120}	r_{240}
f_2	f_2	f_3	f_1	r_{240}	e	r_{120}
f_3	f_3	f_1	f_2	r_{120}	r_{240}	e

As we want a group to model the behaviour of symmetry, we can't just have any set G and any function $\circ : G \times G \to G$. The function $\circ$ must satisfy the same rules that symmetries obey. These are

- Doing nothing is a symmetry.

- The composition of any two symmetries is again a symmetry.
- Every symmetry can be undone by another symmetry.
- Changing the bracketing of composition of multiple symmetries does not affect the result of the composition.

Taking these general rules, we obtain our definition of a group.

Definition 1. *A group is a pair* $(G, \circ)$*, where* G *is a set, and* $\circ : G \times G \to G$ *is a function satisfying the following conditions:*

i) There exists an element $e \in G$ *such that*

$$e \circ g = g = g \circ e$$

for all $g \in G$*.*

ii) For all $g \in G$ *there exists an* $h \in G$ *such that*

$$g \circ h = e.$$

iii) For all $g, h, k \in G$*, we have*

$$(g \circ h) \circ k = g \circ (h \circ k).$$

Lecture 2 (1-9-2023)

In this lecture we will look at several basic examples and non-examples of groups.

Example 1. *Let $G = \{e, r, s\}$ and $\circ : G \times G \to G$ defined by*

$\circ$	e	r	s
e	e	r	s
r	r	s	e
s	s	e	r

We have that condition (i) is satisfied, as from the table, $e \circ g = g = g \circ e$ for all $g \in \{e, r, s\}$.

We have that condition (ii) is satisfied, as we have

$$e \circ e = e$$
$$r \circ s = e$$
$$s \circ r = e.$$

Thus for all $g \in \{e, r, s\}$, there exists $h \in \{e, r, s\}$ such that $g \circ h = e$.

To verify condition (iii), we have to verify that

$$g \circ (h \circ k) = (g \circ h) \circ k$$

for all $g, h, k \in \{e, r, s\}$. This is 27 different equalities we need to check! In the interest of time we will only check 2. You will have to trust me (or verify yourself) that the remaining 25 hold.

First we have that

$$r \circ (r \circ r) = r \circ s = e = s \circ r = (r \circ r) \circ r.$$

Second we have that

$$s \circ (r \circ s) = s \circ e = s = e \circ s = (s \circ r) \circ s.$$

We will now look at a non-example. This example is similar to the last example, but with a different composition.

Example 2. *Let $G = \{e, r, s\}$ and $\circ : G \times G \to G$ defined by*

$\circ$	e	r	s
e	e	r	s
r	r	r	e
s	s	e	s

As in the previous example, we have that condition (i) and (ii) are satisfied. However now when we check condition (iii) we find

$$s \circ (s \circ r) = s \circ e = s \neq e = s \circ r = (s \circ s) \circ r.$$

Hence the composition is not associative, and we do not have a group.

Let us now look at an example where we can completely verify that condition (iii) holds.

Example 3. *Let $G = \mathbb{Z}$ with $n \circ m := n + m$. Here our identity element is going to be 0, so we have $e = 0$. We can now verify condition (i) with a short proof:*

Let $g \in \mathbb{Z}$, then we have

$$g \circ e = g + 0 = g = 0 + g = e \circ g.$$

Given an element $g \in \mathbb{Z}$, we know that $g - g = 0 = e$. Thus the inverse h for this g is going to be $-g$. We can now verify condition (ii) with another short proof:

Let $g \in \mathbb{Z}$, and define $h := -g$. We then have that

$$g \circ h = g + (-g) = 0 = e.$$

Finally we have that condition (iii) holds as addition of integers is associative.

Let $g, h, k \in \mathbb{Z}$, then we have

$$g \circ (h \circ k) = g + (h + k) = (g + h) + k = (g \circ h) \circ k.$$

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

If we replace addition with multiplication in the above example, it is no longer a group.

Example 4. *Let $G = \mathbb{Z}$ with $n \circ m := n \times m$. We have that condition (i) holds with $e = 1$. However condition (ii) fails in general. To see this, consider $g = 2$. Then we need to find an $h \in \mathbb{Z}$ such that*

$$g \circ h = 2 \times h = 1.$$

For this to hold, we must have that $h = \frac{1}{2}$, but then $h \notin \mathbb{Z}$.

If use subtraction as the composition, we also fail to get a group.

Example 5. *Let $G = \mathbb{Z}$ with $n \circ m := n \times m$. We now have that condition (iii) fails in general. Let $g = 2$, $h = 5$, and $k = 7$. Then*

$$g \circ (h \circ k) = 2 - (5 - 7) = 4 \neq -10 = (2 - 5) - 7 = (g \circ h) \circ k.$$

Lecture 3 (6-9-2023)

In this lecture we will prove some general theorems about groups.

Theorem 1. *Let* $(G, \circ)$ *be a group, and let* $g, h, k \in G$ *such that*

$$h \circ g = k \circ g.$$

Then $h = k$.

Proof. We have

$$h = h \circ e = h \circ (g \circ g^{-1}) = (h \circ g) \circ g^{-1} = (k \circ g) \circ g^{-1} = k \circ (g \circ g^{-1}) = k \circ e = k.$$

Thus $h = k$ as claimed. □

Theorem 2. *Let* $(G, \circ)$ *be a group, and let* $\hat{e} \in G$ *such that*

$$\hat{e} \circ g = g = g \circ \hat{e}$$

for all $g \in G$. *Then* $e = \hat{e}$.

Proof. We have

$$e = \hat{e} \circ e$$

as $g = \hat{e} \circ g$ for all $g \in G$, and $e \in G$. We also have

$$\hat{e} \circ e = \hat{e}$$

as e is the identity of $(G, \circ)$. Thus $\hat{e} = e$ as claimed. □

Theorem 3. *Let* $(G, \circ)$ *be a group, and let* $g \in G$. *Then*

$$g^{-1} \circ g = e.$$

Proof. We define $x = g^{-1} \circ g$. We then have

$$\begin{aligned} x &= x \circ e \\ &= x \circ x \circ x^{-1} \\ &= g^{-1} \circ \underbrace{g \circ g^{-1}}_{=e} \circ g \circ x^{-1} \\ &= g^{-1} \circ g \circ x^{-1} \\ &= x \circ x^{-1} \\ &= e. \end{aligned}$$

Thus $g^{-1} \circ g = x = e$ as claimed. □

Theorem 4. *Let $(G, \circ)$ be a group, and let $g, h \in G$ such that*

$$g \circ h = e.$$

Then $h = g^{-1}$.

Proof. We have

$$h = e \circ h = g^{-1} \circ g \circ h = g^{-1} \circ e = g^{-1}.$$

Thus $h = g^{-1}$ as claimed. □

Lecture 4 (8-9-2023)

In this lecture we introduce some new examples of groups.

Definition 2. *Let $N \in \mathbb{N}$. We define*

$$\mathbb{Z}_N := \{0, 1, 2, \cdots, N-1\}$$

and $\circ : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ by

$$a \circ b := \begin{cases} a + b & \textit{if } a + b < N \\ a + b - N & \textit{if } a + b \geq N \end{cases}$$

We can show that $(\mathbb{Z}_N, \circ)$ is a group. Here we show conditions (i) and (ii). Verifying condition (iii) is left as a homework exercise.

Theorem 5. *We have that $(\mathbb{Z}_N, \circ)$ satisfies conditions (i) and (ii) of being a group.*

Proof. (i) : We set $e = 0$. Let $a \in \mathbb{Z}_N$, then $a < N$. Thus $a + 0 < N$, and so

$$a \circ e = a + 0 = a = 0 + a = e \circ a.$$

Hence (i) is satisfied.

(ii) : Let $a \in \mathbb{Z}_N$. We define

$$a^{-1} := \begin{cases} 0 & \text{if } a = 0 \\ N - a & \text{if } a \neq 0 \end{cases}.$$

If $a = 0$, then we have

$$a \circ a^{-1} = 0 \circ 0 = 0 = e.$$

If $a \neq 0$, then we have that

$$a \circ a^{-1} = a + N - a - N = 0 = e.$$

Thus (ii) is satisfied. □

Let us define the above group in a different way, using complex numbers. While the definition has changed. The difference is superficial.

Definition 3. *Let $N \in \mathcal{N}$. We define*

$$\mathbb{Z}_N^{\mathbb{C}} := \{e^{\frac{2\pi i}{N} a} \mid a \in \mathbb{Z}\}$$

and $\circ : \mathbb{Z}_N^{\mathbb{C}} \times \mathbb{Z}_N^{\mathbb{C}} \to \mathbb{Z}_N^{\mathbb{C}}$ by

$$z_1 \circ z_2 := z_1 \times z_2.$$

It is fairly straightforward to show that $(\mathbb{Z}_N^{\mathbb{C}}, \circ)$ is a group.

Theorem 6. *We have that $(\mathbb{Z}_N^{\mathbb{C}}, \circ)$ is a group*

Proof. (i): We set $E = 1 = e^{\frac{2\pi i}{N}0} \in \mathbb{Z}_N^{\mathbb{C}}$. Let $z \in \mathbb{Z}_N^{\mathbb{C}}$, then

$$E \circ z = 1 \times z = z = z \times 1 = z \circ E.$$

Thus (i) is satisfied.

(ii) Let $z \in \mathbb{Z}_N^{\mathbb{C}}$, then $z = e^{\frac{2\pi i}{N}a}$ for some $a \in \mathbb{Z}$. We define $z^{-1} = e^{\frac{2\pi i}{N}(-a)}$. We then have

$$z \circ z^{-1} = e^{\frac{2\pi i}{N}a} \times e^{\frac{2\pi i}{N}(-a)} = e^{\frac{2\pi i}{N}0} = 1 = E.$$

Thus (ii) is satisfied.

(iii) Let $z_1, z_2, z_3 \in \mathbb{Z}_N^{\mathbb{C}}$. Then

$$(z_1 \circ z_2) \circ z_3 = (z_1 \times z_2) \times z_3 = z_1 \times (z_2 \times z_3) = z_1 \circ (z_2 \circ z_3).$$

Thus (iii) is satisfied. □

Lecture 5 (11-9-2023)

In this lecture, we define subgroups and prove some theorems regarding them.

Definition 4. *Let $(G, \circ)$ be a group, and $H \subseteq G$. We say that H is a subgroup of G if*

1) $e \in H$, and

2) $h^{-1} \in H$ for all $h \in H$, and

3) $h_1 \circ h_2 \in H$ for all $h_1, h_2 \in H$.

Some examples of subgroups are as follows:

Example 6. *Consider the group $(\mathbb{Z}_{15}, \circ)$. We have that the subgroups are*

- *$H = \{0\}$,*
- *$H = \{0, 5, 10\}$,*
- *$H = \{0, 3, 6, 9, 12\}$,*
- *$H = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$.*

Any other subset of $\mathbb{Z}_{15}$ is not a subgroup.

While it may seem obvious, we have to show that a subgroup is itself a group.

Theorem 7. *Let $(G, \circ)$ be a group, and H a subgroup of G. Then $(H, \circ)$ is a group.*

Proof. We first have to show that $\circ$ restricts to a function $H \times H \to H$. Let $h_1, h_2 \in H$. Then by (3) we get that $h_1 \circ h_2 \in H$. Thus $\circ : H \times H \to H$ is a function.

By (1) we have that $e \in H$ which we claim is the identity in $(H, \circ)$. Let $h \in H$, then $h \in G$ and so

$$h \circ e = h = e \circ h.$$

Hence condition (i) for a group is satisfied.

Let $h \in H$, then by (2) we get that $h^{-1} \in H$. As $h, h^{-1} \in G$ we have that

$$h \circ h^{-1} = e.$$

Hence condition (ii) for a group is satisfied.

Let $h_1, h_2, h_3 \in H$, then $h_1, h_2, h_3 \in G$. Thus

$$(h_1 \circ h_2) \circ h_3 = h_1 \circ (h_2 \circ h_3).$$

□

We can also prove an alternate critereon for showing a subset of a group is a subgroup.

Theorem 8. *Let $(G, \circ)$ be a group, and $H \subseteq G$. Then H is a subgroup of G if and only if:*

a) $H \neq \emptyset$, and

b) $h_1 \circ h_2^{-1} \in H$ for all $h_1, h_2 \in H$.

Proof. First suppose that H is a subgroup, so conditions (1), (2), and (3) hold. From (1) we get that $e \in H$, so $H \neq \emptyset$. Thus (a) holds.

Let $h_1, h_2 \in H$, then from (2) we have that $h_2 \in H$, and so (3) gives that $h_1 \circ h_2^{-1} \in H$. Hence (b) holds.

Now suppose that (a) and (b) hold. From (a) we have that $H \neq \emptyset$, so there exists $h \in H$. Thus from (b) we get that

$$e = h \circ h^{-1} \in H$$

and so (1) holds.

Let $h \in H$. We have shown that $e \in H$, so from (b) we get

$$h^{-1} = e \circ h^{-1} \in H.$$

Hence (2) holds.

Let $h_1, h_2 \in H$. We have shown that $h_2^{-1} \in H$. Hence (b) gives that

$$h_1 \circ h_2 = h_1 \circ (h_2^{-1})^{-1} \in H.$$

Thus (3) holds, and so H is a subgroup. □

Lecture 6 (13-9-2023)

In this lecture we define a new family of groups.

Definition 5. *Let $N \in \mathbb{N}_{N\geq 1}$. We define*

$$S_N := \{f : \{1, 2, \cdots, N\} \to \{1, 2, \cdots, N\} \mid \ f \textit{ is a bijection}\}$$

As the composition of two bijections is again a bijection, we have that function composition is a function $\circ : S_N \times S_N \to S_N$.

We will use the convention that

$$(f_1 \circ f_2)(x) := f_2(f_1(x)).$$

We then have that $(S_N, \circ)$ is group.

Theorem 9. *For all $N \in \mathbb{N}_{N\geq 1}$ we have that $(S_N, \circ)$ is a group.*

Proof. We will first prove associativity. Let $f_1, f_2, f_3 \in S_N$, and let $x \in \{1, 2, \cdots, N\}$. We then have

$$(f_1 \circ (f_2 \circ f_3))(x) = (f_2 \circ f_3)(f_1(x)) = f_3(f_2(f_1(x))),$$

and

$$((f_1 \circ f_2) \circ f_3)(x) = f_3((f_1 \circ f_3)(x)) = f_3(f_2(f_1(x))).$$

Thus $((f_1 \circ f_2) \circ f_3)(x) = (f_1 \circ (f_2 \circ f_3))(x)$ for all $x \in \{1, 2, \cdots, N\}$, hence $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$. Thus condition (iii) is satisfied.

To show condition (i), we define $\mathrm{id}_N \in S_N$ by $\mathrm{id}_N(x) := x$, and claim this is the group identity. To see this let $f \in S_N$, and $x \in \{1, 2, \cdots, N\}$. We then have

$$(f \circ \mathrm{id}_N)(x) = \mathrm{id}_N(f(x)) = f(x) = f(\mathrm{id}_N(x)) = (\mathrm{id}_N \circ f)(x).$$

Hence $f \circ \mathrm{id}_N = f = \mathrm{id}_N \circ f$. Thus condition (i) holds.

We finish by showing (ii) holds. Let $f \in S_N$, then f is a bijection. To define f^{-1} we let $y \in \{1, 2, \cdots, N\}$. As f is surjective, there exists $x_y \in \{1, 2, \cdots, N\}$ such that

$$f(x_y) = y.$$

As f is surjective, this x_y is unique. We define the function f^{-1} by

$$f^{-1}(y) = x_y.$$

We claim that $f^{-1} \in S_N$, i.e. that f^{-1} is bijective.

Inj) Let $y_1, y_2 \in \{1, 2, \cdots, N\}$ such that $f^{-1}(y_1) = f^{-1}(y_2)$. Then $x_{y_1} = x_{y_2}$, and so

$$y_1 = f(x_{y_1}) = f(x_{y_2}) = y_2.$$

Hence f^{-1} is injective.

Sur) Let $x \in \{1, 2, \cdots, N\}$, and define $y = f(x)$. We claim that $f^{-1}(y) = x$. To see this note that $f^{-1}(y) = x_y$, and that $f(x_y) = y$. We then have $f(x_y) = y = f(x)$, hence $x_y = x$ as f is injective. Thus $f^{-1}(y) = x_y = x$ and so f^{-1} is surjective.

Thus $f^{-1} \in S_N$. We now have to show that $f^{-1} \circ f = \mathrm{id}_N$. To see this let $y \in \{1, 2, \cdots, N\}$. We then have

$$(f^{-1} \circ f)(y) = f(f^{-1}(y)) = f(x_y) = y = \mathrm{id}_N(y).$$

Hence $f^{-1} \circ f = \mathrm{id}_N$ and so (ii) is satisfied. □

Lecture 7 (15-9-2023)

In this lecture we will build towards proving that the number of elements in a subgroup divides the number of elements in a group. We will prove this using cosets.

Definition 6. *Let $(G, \circ)$ be a group, and H a subgroup of G. For all $g \in G$ we define*

$$gH := \{g \circ h \mid h \in H\}.$$

These subsets of G are called the left cosets of H.

The following theorem gives a convenient characterisation of when two cosets are equal.

Theorem 10. *Let $(G, \circ)$ be a group, H a subgroup of G, and $g_1, g_2 \in G$. Then we have*

$$g_1H = g_2H \iff g_2^{-1} \circ g_1 \in H.$$

Proof. $\implies$) Assume $g_1H = g_2H$. As $e \in H$, we have that $g_1 = g_1 \circ e \in g_1H$. Thus $g_1 \in g_2H$, and so there exists $h \in H$ such that $g_1 = g_2 \circ h$. By left composing by g_2^{-1} we then get $g_2^{-1} \circ g_1 = h \in H$.

$\impliedby$) Assume $g_2^{-1} \circ g_1 \in H$. We will show that $g_1H = g_2H$.

$\subseteq$) Let $x \in g_1H$, then there exists $h \in H$ such that $x = g_1 \circ h$. Thus

$$x = g_2 \circ g_2^{-1} \circ g_1 \circ h.$$

As $g_2^{-1} \circ g_1 \in H$ and $h \in H$, we get $g_2^{-1} \circ g_1 \circ h \in H$. Hence $x \in g_2H$.

$\supseteq$) Let $x \in g_2H$, then there exists $h \in H$ such that $x = g_2 \circ h$. Thus

$$x = g_1 \circ g_1^{-1} \circ g_2 \circ h.$$

As $g_2^{-1} \circ g_1 \in H$, we get that $g_1^{-1} \circ g_2 = (g_2^{-1} \circ g_1)^{-1} \in H$. Hence $g_1^{-1} \circ g_2 \circ h \in H$ and so $x \in g_1H$.

Together we get $g_1H = g_2H$. □

We can now quickly prove that cosets are either equal or disjoint.

Theorem 11. *Let $(G, \circ)$ be a group, H a subgroup of G. Then for all $g_1, g_2 \in G$ we have either*

$$g_1H = g_2H \quad \text{or} \quad g_1H \cap g_2H = \emptyset.$$

Proof. We either have that $g_1H \cap g_2H = \emptyset$ or $g_1H \cap g_2H \neq \emptyset$.

If $g_1H \cap g_2H = \emptyset$ we are done.

If $g_1 H \cap g_2 H \neq \emptyset$, then there exists $x \in g_1 H \cap g_2 H$. Hence there exists $h_1, h_2 \in H$ such that $x = g_1 \circ h_1$ and $x = g_2 \circ h_2$. Thus

$$\begin{aligned} g_1 \circ h_1 = g_2 \circ h_2 &\implies g_2^{-1} \circ g_1 \circ h_1 = h_2 \\ &\implies g_2^{-1} \circ g_1 = h_2 \circ h_1^{-1} \in H. \end{aligned}$$

Therefore $g_1 H = g_2 H$ by Theorem 10. □

Lecture 8 (18-9-2023)

In this lecture we finish our proof that the number of elements of a subgroup divide the number of elements of the group. We begin by showing that there is bijection between any two cosets of a subgroup.

Theorem 12. *Let $(G, \circ)$ be a group, H a subgroup of G. Then for all $g_1, g_2 \in G$ there exists a bijection $g_1H \to g_2H$.*

Proof. Let $x \in g_1H$. We define

$$f(x) = g_2 g_1^{-1} x.$$

As $x = g_1h$ for some $h \in H$, we have that $f(x) = g_2g_1^{-1}g_1h = g_2h \in g_2H$. Therefore $f(x) \in g_2H$ and f is a function $g_1H \to g_2H$.

We next claim that f is a bijection.

inj) Let $x_1, x_2 \in g_1H$ such that $f(x_1) = f(x_2)$. Then we have

$$\begin{aligned} g_2g_1^{-1}x_1 = g_2g_1^{-1}x_2 &\implies g_1^{-1}x_1 = g_1^{-1}x_2 \\ &\implies x_1 = x_2. \end{aligned}$$

Thus f is injective.

sur) Let $y \in g_2H$. Then there exists $h \in H$ such that $y = g_2h$. We define

$$x = g_1h \in g_1H.$$

We then have

$$f(x) = g_2g_1^{-1}g_1h = g_2h = y.$$

Thus f is bijective. □

We can now show that the cosets of H form a partition of G. Let us first recall the definition of a partition.

Definition 7. *Let X be a set. A partition of X is a collection of subsets $X_i \subseteq X$ such that:*

a) $\bigcup_i X_i = X$, and

b) $X_i \cap X_j = \emptyset$ if $i \neq j$.

Note that if X is a finite set we have that

$$|X| = \sum_i |X_i|.$$

Theorem 13. *Let $(G, \circ)$ be a group, H a subgroup of G. Then*

$$\{gH \mid g \in G\}$$

is a partition of G.

Proof. We claim that

$$\bigcup_{g\in G} gH = G.$$

$\subseteq$) As each $gH \subseteq G$, we have that $\bigcup_{g\in G} gH \subseteq G$.

$\supseteq$) Let $g \in G$, then $g = g \circ e \in gH$, and so $g \in \bigcup_{g\in G} gH$. Therefore $G \subseteq \bigcup_{g\in G} gH$.

Together we get that $\bigcup_{g\in G} gH = G$ as desired, and so condition a) for a partition holds.

From Theorem 11 we have that condition b) holds. □

We can now prove the main theorem.

Theorem 14. *Let $(G, \circ)$ be a finite group, H a subgroup of G. Then*

$$|H| \mid |G|.$$

Proof. By Theorem 13 we have that

$$\{gH \mid g \in G\}$$

is a partition of G. Therefore

$$\begin{aligned}|G| &= |H| + |g_2H| + |g_3H| + \cdots + |g_nH| \\ &= |H| + |H| + |H| + \cdots + |H| \\ &= n|H|.\end{aligned}$$

Thus $|H| \mid |G|$. □

Lecture 9 (20-9-2023)

In this lecture we introduce a new family of groups.

Definition 8. *Let $N \in \mathbb{N}$. We define*

$$GL(N) := \{M \in M_n(\mathbb{C}) \mid \det(A) \neq 0\}.$$

In the case that $N = 1$, we have that $GL(N) = \mathbb{C} - \{0\}$.

In the case that $N = 2$, we have that

$$GL(2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{C} \text{ such that } ad \neq bc \right\}.$$

We can prove that $GL(N)$ is a group with composition given by matrix multiplication.

Theorem 15. *Let $N \in \mathbb{N}$. Then $(GL(N), \cdot)$ is a group.*

Proof. We first show that matrix multiplication is a function $GL(N) \times GL(N) \to GL(N)$. Let $M_1, M_2 \in GL(N)$, then $\det(M_1) \neq 0$ and $\det(M_2) \neq 0$. Thus

$$\det(M_1 \cdot M_2) = \det(M_1) \times \det(M_2) \neq 0.$$

Hence $M_1 \cdot M_2 \in GL(N)$.

We now check the three conditions required to be a group.

i) We claim that the $N \times N$ identity matrix I_N is the group identity. Let $M \in GL(N)$, then

$$I_N \cdot M = M = M \cdot I_N.$$

Hence condition (i) is satisfied.

ii) Let $M \in GL(N)$, then $\det(M) \neq 0$. Thus there exists $M^{-1} \in M_n(\mathbb{C})$ such that

$$M \cdot M^{-1} = I_N.$$

We have

$$\det(M^{-1}) = \frac{1}{\det M} \neq 0.$$

Thus $M^{-1} \in GL(N)$.

iii) We have that matrix multiplication is associative, hence (iii) holds. □

Let's find a subgroup of $GL(N)$.

Exercise 1. *Show that*

$$SL(N) := \{M \in M_n(\mathbb{C}) \mid \det(A) = 1\}$$

is a subgroup of $GL(N)$.

Solution. *We have that* $\det(I_N) = 1$*, thus* $SL(N) \neq \emptyset$*.*

Let $M_1, M_2 \in SL(N)$*. Then* $\det(M_1) = 1 = \det(M_2)$*. Thus*

$$\det(M_1 \cdot M_2^{-1}) = \frac{\det(M_1)}{\det(M_2)} = 1.$$

Hence $M_1 \cdot M_2^{-1} \in SL(N)$ *and so* $SL(N)$ *is a subgroup of* $GL(N)$*.*

We have that every finite group G is a subgroup of $GL(|G|)$. The identification of g with a $|G| \times |G|$ matrix M^g is as follows:

First order the elements of the group G as $\{g_1, g_2, \cdots, g_{|G|}\}$. We then define

$$M^g_{i,j} := \begin{cases} 1 & \text{if } g \circ g_i = g_j \\ 0 & \text{otherwise} \end{cases}$$

The group $GL(N)$ also has many subgroups with order larger (and smaller) than N.

Exercise 2. *Find a subgroup* H *of* $GL(2)$ *such that there exists elements* $r \in H$ *and* $s \in H$ *satisfying the relations*

$$s^2 = e, \qquad r^3 = e, \qquad sr = r^2 s.$$

How many elements are in H*?*

Solution. *By choosing a suitable basis, we may assume* r *is of the form*

$$r = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

As $r^3 = e$*, we get that*

$$\begin{bmatrix} \lambda_1^3 & 0 \\ 0 & \lambda_2^3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus $\lambda_1^3 = 1 = \lambda_2^3$*, and so*

$$\lambda_1, \lambda_2 \in \{1, e^{2\pi i \frac{1}{3}}, e^{2\pi i \frac{2}{3}}\}.$$

We have that s *is of the form*

$$s = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

As $s^2 = e$ *we get*

$$\begin{bmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

As $sr = r^2 s$ *we get*

$$\begin{bmatrix} a\lambda_1 & b\lambda_2 \\ c\lambda_1 & d\lambda_2 \end{bmatrix} = \begin{bmatrix} a\lambda_1^2 & b\lambda_1^2 \\ c\lambda_2^2 & d\lambda_2^2 \end{bmatrix}.$$

Thus we have

- *Either* $\lambda_1 = 1$ *or* $a = 0$*,*
- *Either* $\lambda_2 = \lambda_1^2$ *or* $b = 0$*,*
- *Either* $\lambda_1 = \lambda_2^2$ *or* $c = 0$*,*
- *Either* $\lambda_2 = 1$ *or* $d = 0$*.*

We then have several cases:

Case $\lambda_1 = 1 = \lambda_2$*: In this case we have that* $e = r$*, so we can rule this case out.*

Case $\lambda_1 = 1$ *and* $\lambda_2 \neq 1$*: As* $\lambda_2 \neq 1$*, we get* $d = 0$*. From* $d^2 + bc = 1$ *we then have* $bc = 1$*, and so both* b *and* c *are non-zero. Thus* $\lambda_2 = \lambda_1^2 = 1$ *which contradicts* $\lambda_2 \neq 1$*. This rules this case out.*

Case $\lambda_1 \neq 1$ *and* $\lambda_2 = 1$*: This case is ruled out in the same manner as the previous case.*

Case $\lambda_1 \neq 1$ *and* $\lambda_2 \neq 1$*: In this case we must have* $a = 0 = d$*. Thus* $bc = 1$*, so* $c = \frac{1}{b}$*, which implies that* $\lambda_2 = \lambda_1^2$*. We thus get a particular solution:*

$$r = \begin{bmatrix} e^{2\pi i \frac{1}{3}} & 0 \\ 0 & e^{2\pi i \frac{2}{3}} \end{bmatrix} \quad \text{and } s = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Direct computation shows that H *then has 6 elements.*

Lecture 10 (22-9-2023)

In this lecture we introduce the notion of group homomorphisms between groups. These are functions which preserve the group structure.

Definition 9. *Let $(G_1, \circ)$ and $(G_2, *)$ be groups. A group homomorphism $f : G_1 \to G_2$ is a function $f : G_1 \to G_2$ such that*

$$f(g_1 \circ g_2) = f(g_1) * f(g_2)$$

for all $g_1, g_2 \in G_1$. If f is a bijection, we call it an isomorphism.

We have the following examples.

Example 7. *Let $G_1 = \mathbb{Z}_9$ and $G_2 = \mathbb{Z}_3$. Then the function*

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(2) &= 2 \\ f(3) &= 0 \\ f(4) &= 1 \\ f(5) &= 2 \\ f(6) &= 0 \\ f(7) &= 1 \\ f(8) &= 2 \end{aligned}$$

is a group homomorphism $G_1 \to G_2$, as we have $f(a \circ b) = f(a) \circ f(b)$ for all $a, b \in \mathbb{Z}_9$. To demonstrate one of these, we have

$$f(6 \circ 7) = f(4) = 1 = 0 \circ 1 = f(6) \circ f(7).$$

Example 8. *Let $G_1 = GL(N)$ and $G_2 = \mathbb{C} - \{0\}$. The composition on G_2 is multiplication. We have that* $\det : GL(N) \to \mathbb{C} - \{0\}$ *is a group homomorphism as*

$$\det(M_1 \cdot M_2) = \det(M_1) \times \det(M_2)$$

for all $M_1, M_2 \in GL(N)$.

We end with the following exercise.

Exercise 3. *Find all group homomorphisms $\mathbb{Z}_6$ to $\mathbb{Z}_3$.*

Solution. *We must have that $f(0) = 0$ for any group homomorphism. We then have three possibilities for $f(1)$, which can be 0, 1, or 2.*

***Case** $f(1) = 0$**:** In this case we then have that*

$$f(2) = f(1 \circ 1) = f(1) \circ f(1) = 0 \circ 0 = 0.$$

In the same fashion we get that

$$f(3) = f(1) \circ f(2) = 0 \circ 0 = 0.$$

Carrying on with this logic gives that

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 0 \\ f(2) &= 0 \\ f(3) &= 0 \\ f(4) &= 0 \\ f(5) &= 0 \end{aligned}$$

Case $f(1) = 1$***:*** *In this case we then have that*

$$f(2) = f(1 \circ 1) = f(1) \circ f(1) = 1 \circ 1 = 2.$$

In the same fashion we get that

$$f(3) = f(1) \circ f(2) = 1 \circ 2 = 0.$$

Carrying on with this logic gives that

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(2) &= 2 \\ f(3) &= 0 \\ f(4) &= 1 \\ f(5) &= 2 \end{aligned}$$

Case $f(1) = 2$***:*** *In this case we then have that*

$$f(2) = f(1 \circ 1) = f(1) \circ f(1) = 2 \circ 2 = 1.$$

In the same fashion we get that

$$f(3) = f(1) \circ f(2) = 2 \circ 1 = 0.$$

Carrying on with this logic gives that

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 2 \\ f(2) &= 1 \\ f(3) &= 0 \\ f(4) &= 2 \\ f(5) &= 1 \end{aligned}$$

Lecture 11 (25-9-2023)

In this lecture we will prove some theorems regarding group homomorphisms.

Theorem 16. *Let $(G_1, \circ)$ and $(G_2, *)$ be groups, and $f : G_1 \to G_2$ a group homomorphism. Then*

a) $f(e_{G_1}) = e_{G_2}$,

b) $f(g)^{-1} = f(g^{-1})$.

Proof. a) We have

$$\begin{aligned} e_{G_2} &= f(e_{G_1})^{-1} * f(e_{G_1}) \\ &= f(e_{G_1})^{-1} * f(e_{G_1} \circ e_{G_1}) \\ &= f(e_{G_1})^{-1} * f(e_{G_1}) * f(e_{G_1}) \\ &= e_{G_2} * f(e_{G_1}) \\ &= f(e_{G_1}). \end{aligned}$$

Thus $f(e_{G_1}) = e_{G_2}$ as claimed.

b) Let $g \in G_1$. Then we have

$$e_{G_2} = f(e_{G_1}) = f(g \circ g^{-1}) = f(g) * f(g^{-1}).$$

Thus $f(g)^{-1} = f(g^{-1})$ as claimed. □

We now define the kernel and image of a group homomorphism.

Definition 10. *Let $(G_1, \circ)$ and $(G_2, *)$ be groups, and $f : G_1 \to G_2$ a group homomorphism. We define*

$$\begin{aligned} \operatorname{im}(f) &:= \{f(g) \mid g \in G_1\} \subseteq G_2 \\ \ker(f) &:= \{g \mid f(g) = e_{G_2}\} \subseteq G_1. \end{aligned}$$

Lets work a quick example to understand these definitions.

Example 9. *Let $G_1 = \mathbb{Z}$ with addition at the group operation, and $G_2 = \mathbb{Z}_2$. Then*

$$f(n) = \begin{cases} 0 & n \text{ is even} \\ 1 & n \text{ is odd} \end{cases}$$

is a group homomorphism. We have that

$$\operatorname{im}(f) = \{0, 1\},$$

and

$$\ker(f) = \{2n \mid n \in \mathbb{Z}\}.$$

We can prove that $\ker(f)$ is always a subgroup of G_1.

Theorem 17. *Let $(G_1, \circ)$ and $(G_2, *)$ be groups, and $f : G_1 \to G_2$ a group homomorphism. Then $\ker(f)$ is a subgroup of G_1.*

Proof. As $f(e_{G_1}) = e_{G_2}$ we have that $e_{G_1} \in \ker(f)$, and so $\ker(f) \neq \emptyset$.

Let $g_1, g_2 \in \ker(f)$, then

$$f(g_1) = e_{G_2} = f(g_2).$$

Therefore

$$f(g_1 \circ g_2^{-1}) = f(g_1) * f(g_2)^{-1} = e_{G_2} * e_{G_2}^{-1} = e_{G_2}.$$

Hence $g_1 \circ g_2^{-1} \in \ker(f)$.

Thus $\ker(f)$ is a subgroup of G_1 by Theorem 8. □

Our final theorem of the day will show that a homomorphism f is injective exactly when its kernel just contains the identity.

Theorem 18. *Let $(G_1, \circ)$ and $(G_2, *)$ be groups, and $f : G_1 \to G_2$ a group homomorphism. Then f is injective if and only if $\ker(f) = \{e_{G_1}\}$.*

Proof. $\Longrightarrow$) Assume f is injective, and let $g \in \ker(f)$. Then $f(g) = e_{G_2} = f(e_{G_1})$. As f is injective, we get that $g = e_{G_1}$, and so $\ker(f) = \{e_{G_1}\}$.

$\Longleftarrow$) Assume $\ker(f) = \{e_{G_1}\}$ and let $g_1, g_2 \in G_1$ such that $f(g_1) = f(g_2)$. We then have

$$\begin{aligned}
& f(g_1) * f(g_2)^{-1} = e_{G_2} \\
\Longrightarrow\ & f(g_1 \circ g_2^{-1}) = e_{G_2} \\
\Longrightarrow\ & g_1 \circ g_2^{-1} \in \ker(f) \\
\Longrightarrow\ & g_1 \circ g_2^{-1} = e_{G_1} \\
\Longrightarrow\ & g_1 = g_2.
\end{aligned}$$

Hence f is injective. □

Lecture 12 (27-9-2023)

In this lecture we define a new construction for producing examples of groups.

Definition 11. *Let G and H be groups. We define a composition $\circ$ on $G \times H$ by*

$$(g_1, h_1) \circ (g_2, h_2) := (g_1 g_2, h_1, h_2).$$

We then have that $G \times H$ is a group with this new composition.

Theorem 19. *Let G and H be groups. Then $(G \times H, \circ)$ is a group.*

Proof. i) We claim that (e_G, e_H) is the identity. Let $(g, h) \in G \times H$, then

$$\begin{aligned}(e_G, e_H) \circ (g, h) &= (e_G g, e_H h)\\ &= (g, h)\\ &= (g e_G, h e_H)\\ &= (g, h) \circ (e_G, e_H).\end{aligned}$$

Thus condition i) holds.

ii) Let $(g, h) \in G \times H$. We claim that $(g^{-1}, h^{-1}) \in G \times H$ is the inverse of (g, h). To see this we compute

$$(g, h) \circ (g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H).$$

Thus condition ii) holds.

iii) Let $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$. Then we have

$$\begin{aligned}(g_1, h_1) \circ ((g_2, h_2) \circ (g_3, h_3)) &= (g_1, h_1) \circ (g_2 g_3, h_2 h_3)\\ &= (g_1(g_2 g_3), h_1(h_2 h_3))\\ &= ((g_1 g_2) g_3, (h_1 h_2) h_3)\\ &= (g_1 g_2, h_1 h_2) \circ (g_2, h_3)\\ &= ((g_1, h_1) \circ (g_2, h_2)) \circ (g_3, h_3).\end{aligned}$$

Thus condition (iii) holds, and so $G \times H$ is a group. □

The group $G \times H$ is called the *direct product* of G and H. We have already seen some examples of direct products.

Example 10. *The group $\mathbb{Z}_{15}$ is isomorphic to the direct product $\mathbb{Z}_3 \times \mathbb{Z}_5$.*

However not every group is a direct product of two smaller groups.

Example 11. *There is not an isomorphism between $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

We desire a result that exactly tells us when a group G can be written as a direct product of smaller groups. For this we need to introduce *normal subgroups*.

Definition 12. *Let G a group, and H a subgroup of G. We say that H is a normal subgroup if*

$$ghg^{-1} \in H$$

for all $g \in G$ and $h \in H$.

We have the following example.

Example 12. *The subgroup $SL(N) := \{M \in GL(N) \mid \det(M) = 1\}$ of $GL(N)$ from Exercise 1 is a normal subgroup. This is because for all $g \in GL(N)$ and $h \in SL(N)$ we have that*

$$\det(ghg^{-1}) = \det(g)\det(h)\det(g)^{-1} = 1.$$

Thus $ghg^{-1} \in SL(N)$.

Lecture 13 (29-9-2023)

In this lecture we will prove a characterisation of when a group is the direct product of two subgroups, and define a new family of finite groups.

Theorem 20. *Let G a group, and H_1, H_2 normal subgroups of G. If*

$$H_1 \cap H_2 = \{e\} \quad \text{and} \quad H_1 H_2 = G$$

then $G \cong H_1 \times H_2$.

Before we can prove this, we first need to prove the following intermediate result.

Lemma 1. *Let G a group, and H_1, H_2 normal subgroups of G such that*

$$H_1 \cap H_2 = \{e\}.$$

Then for all $h_1 \in H_1$ and $h_2 \in H_2$ we have that

$$h_1 h_2 = h_2 h_1.$$

Proof. We consider the element $h_1 h_2 h_1^{-1} h_2^{-1}$. As $h_2 \in H_2$, and $h_1 \in G$, we get that $h_1 h_2 h_1^{-1} \in H_2$ as H_2 is normal. As subgroups are closed under inverses and compositions we then get

$$h_1 h_2 h_1^{-1} h_2^{-1} \in H_2.$$

On the other hand, as $h_1^{-1} \in H_1$ and $h_2 \in G$, we get that $h_2 h_1^{-1} h_2^{-1} \in H_1$ as H_1 is normal. Thus we have

$$h_1 h_2 h_1^{-1} h_2^{-1} \in H_1.$$

Together we get

$$h_1 h_2 h_1^{-1} h_2^{-1} \in H_1 \cap H_2 = \{e\}$$

and so $h_1 h_2 h_1^{-1} h_2^{-1} = e$ which implies that $h_1 h_2 = h_2 h_1$. □

We can now prove Theorem 20.

Proof of Theorem 20. We define a function $f : H_1 \times H_2 \to G$ by

$$f((h_1, h_2)) = h_1 h_2.$$

We claim that f is an isomorphism.

Homomorphism) Let $(h_1, h_2), (h_3, h_4) \in H_1 \times H_2$, then we have

$$\begin{aligned} f((h_1, h_2) \circ (h_3, h_4)) &= f((h_1 h_3, h_2 h_4)) \\ &= h_1 h_3 h_2 h_4 \\ &= h_1 h_2 h_3 h_4 \quad \text{by Lemma 1} \\ &= f((h_1, h_2)) f((h_3, h_4)). \end{aligned}$$

Thus f is a homomorphism.

Injectivity) Let $(h_1, h_2) \in \ker(f)$, then $e = f((h_1, h_2)) = h_1 h_2$. Thus $h_2 = h_1^{-1} \in H_1$, and so $h_2 \in H_1 \cap H_2 = \{e\}$. Thus $h_2 = e$ which implies that $h_1 = e$. Therefore $\ker(f) = \{(e, e)\}$ which gives that f is injective by Theorem 18.

Surjectivity) Let $g \in G = H_1 H_2$, then there exists $h_1 \in H_1$ and $h_2 \in H_2$ such that $g = h_1 h_2$. Therefore

$$f((h_1, h_2)) = h_1 h_2 = g.$$

Hence f is surjective. □

For the second part of the lecture introduce a new family of groups. These groups will describe the symmetries of the $N - gon$.

Definition 13. *Let $N \in \mathbb{N}_{\geq 2}$ and define*

$$D_N := \langle r, s \mid r^N = e, s^2 = e, sr = r^{N-1}s\rangle$$

By this notation we mean the group consisting of all possible compositions of r and s (i.e. $rs^4r^3sr^7$) with the equations $r^N = e$, $s^2 = e$, and $sr = r^{N-1}s$ applied. For example if $N = 6$ we would have

$$\begin{aligned} rs^4r^3sr^7 &= rs^4r^3srr^6 \\ &= rs^4r^3sre \\ &= rs^4r^3sr \\ &= rer^3sr \\ &= r^4sr \\ &= r^4r^5s \\ &= r^9s \\ &= r^3s \end{aligned}$$

The elements of D_N are as follows:

$$D_N = \{e, r, r^2, \cdots, r^{N-1}, s, rs, r^2s, \cdots, r^{N-1}s\}.$$

The compositions between all of these elements can all be determined by the three equations $r^N = e$, $s^2 = e$, and $sr = r^{N-1}s$. For example

$$r^2s \circ r^2s = r^2srrs = r^2r^{N-1}srs = r^2r^{N-1}r^{N-1}ss = r^{2N}s^2 = e.$$

Lecture 14 (1-10-2023)

In this lecture we will work over some exam style questions.

For the following questions no justification is required.

Exercise 4. *Give an example of a homomorphism* $f : D_4 \to D_8$ *with* $\ker(f) = \{e\}$.

Solution.

$$\begin{aligned} e &\mapsto e \\ r &\mapsto r^2 \\ r^2 &\mapsto r^4 \\ r^3 &\mapsto r^6 \\ s &\mapsto s \\ rs &\mapsto r^2 s \\ r^2 s &\mapsto r^4 s \\ r^3 s &\mapsto r^6 s \end{aligned}$$

Exercise 5. *List the elements of* S_3

Solution.

$$S_3 = \{(), (12), (23), (13), (123), (132)\}$$

Exercise 6. *Let* $H = \{(), (13)\} \subseteq S_3$. *List the left cosets of* H.

Solution.

$$\begin{aligned} &\{(), (13)\} \\ &\{(12), (123)\} \\ &\{(23), (132)\} \end{aligned}$$

Exercise 7. *Let* $G = \mathbb{Z}$ *with operation given by addition, and let* $f : G \to G$ *be defined by* $f(n) = 6n$. *Determine* $\ker(f)$.

Solution.

$$\ker(f) = \{0\}.$$

Exercise 8. *We define* $a \circ : (\mathbb{R} - \{0\}) \times (\mathbb{R} - \{0\}) \to (\mathbb{R} - \{0\})$ *by* $a \circ b = 4ab$. *Show that* $(\mathbb{R} - \{0\}, \circ)$ *is a group. You must justify your answer.*

Solution. *We claim that* $\frac{1}{4}$ *is the identity. Let* $a \in (\mathbb{R} - \{0\})$. *Then*

$$a \circ \frac{1}{4} = 4a\frac{1}{4} = a = 4\frac{1}{4}a = \frac{1}{4} \circ a.$$

Thus condition i) holds.

Let $a \in (\mathbb{R} - \{0\})$. We claim that $a^{-1} = \frac{1}{16a}$. Indeed we have

$$a \circ a^{-1} = 4a\frac{1}{16a} = \frac{1}{4}.$$

Thus condition ii) holds.

Let $a, b, c \in (\mathbb{R} - \{0\})$, then we have

$$a \circ (b \circ c) = a \circ (4bc) = 16abc$$

and

$$(a \circ b) \circ c = (4ab) \circ c = 16abc.$$

Thus $a \circ (b \circ c) = (a \circ b) \circ c$ and so condition iii) holds. Thus $(\mathbb{R} - \{0\}, \circ)$ is a group.

Exercise 9. *Show that*

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \mid a \in \mathbb{R} - \{0\} \right\} \subset GL(2)$$

is a subgroup of $GL(2)$.

Solution. *As $1 \in \mathbb{R} - \{0\}$ we have that*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \mid a \in \mathbb{R} - \{0\} \right\}$$

and so this subset is non-empty.

Let

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix} \in \left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \mid a \in \mathbb{R} - \{0\} \right\}.$$

We then have $\begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} b^{-1} & 0 \\ 0 & b \end{bmatrix}$ and so

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} ab^{-1} & 0 \\ 0 & a^{-1}b \end{bmatrix} = \begin{bmatrix} ab^{-1} & 0 \\ 0 & (ab^{-1})^{-1} \end{bmatrix}.$$

As $ab^{-1} \in \mathbb{R} - \{0\}$, we get that

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}^{-1} \in \left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \mid a \in \mathbb{R} - \{0\} \right\}$$

and so

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \mid a \in \mathbb{R} - \{0\} \right\}$$

is a subgroup of $GL(2)$.

Lecture 15 (6-10-2023)

In this lecture we will do some revision style questions.

Exercise 10. *Show that $H := \{e, r, \cdots, r^{n-1}\}$ is a normal subgroup of D_n.*

Solution. *To show H is a subgroup, we first observe that $H \neq \emptyset$ as $e \in H$. Now let $h_1, h_2 \in H$, then by definition there exist $n_1, n_2 \in \mathbb{Z}$ such that $h_1 = r^{n_1}$ and $h_2 = r^{n_2}$. We then have*

$$h_1 h_2^{-1} = r^{n_1} r^{-n_2} = r^{n_1 - n_2} \in H.$$

Thus H is a subgroup of D_n.

To show that H is normal let $h \in H$ and $g \in D_n$. Then $h = r^k$ for some $k \in \mathbb{Z}$ and we have that either $g = r^l$ or $g = sr^l$ for some $l \in \mathbb{Z}$.

In the case that $g = r^l$ we have

$$ghg^{-1} = r^l r^k r^{-l} = r^k \in H.$$

In the case that $g = sr^l$ we have

$$ghg^{-1} = sr^l r^k (sr^l)^{-1} = sr^{l+k} sr^l = s^2 r^{-l-k} r^l = r^{-k} \in H.$$

In all cases we have $ghg^{-1} \in H$, so H is normal.

Exercise 11. *Let G be a group such that*

$$(ab)^2 = a^2 b^2$$

for all $a, b \in G$. Show that

$$ab = ba$$

for all $a, b \in G$.

Solution. *Let $a, b \in G$, then*

$$\begin{aligned} &abab = (ab)^2 = a^2 b^2 = aabb \\ \implies &bab = abb \\ \implies &ba = ab. \end{aligned}$$

Exercise 12. *Find a subgroup H of $GL(2)$ with 3 elements*

Solution. *We have that H must be of the form*

$$H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, M, M^{-1} \right\}$$

with $M^2 = M^{-1}$. Equivalently, we need $M^3 = I_2$. There are many such matrices. One is

$$\begin{bmatrix} e^{2\pi i \frac{1}{3}} & 0 \\ 0 & e^{2\pi i \frac{1}{3}} \end{bmatrix}.$$

Thus

$$H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} e^{2\pi i \frac{1}{3}} & 0 \\ 0 & e^{2\pi i \frac{1}{3}} \end{bmatrix}, \begin{bmatrix} e^{2\pi i \frac{2}{3}} & 0 \\ 0 & e^{2\pi i \frac{2}{3}} \end{bmatrix} \right\}$$

Exercise 13. *Let G be a group. Show that $f : G \to G \times G$ defined by $f(g) = (g, g)$ is a homomorphism.*

Solution. *Let $g_1, g_2 \in G$, then*

$$f(g_1)f(g_2) = (g_1, g_1)(g_2, g_2) = (g_1g_2, g_1g_2) = f(g_1g_2).$$

Thus f is a homomorphism.

Lecture 16 (11-10-2023)

In this lecture we will introduce the automorphism group of a group. This is a method of constructing another group from a given group.

Definition 14. *Let G be a group. We define*

$$\mathrm{Aut}(G) := \{f : G \to G \mid f \text{ is an isomorphism } \}.$$

The goal of todays lecture is to prove that $\mathrm{Aut}(G)$ is a group with operation given by function composition.

Let's start by working an example.

Example 13. *Let $N \in \mathbb{N}_{\geq 1}$ and consider $G = \mathbb{Z}_N$. Any homomorphism $\mathbb{Z}_N \to \mathbb{Z}_N$ is determined by where it sends 1. We therefore have that the homomorphisms $\mathbb{Z}_N \to \mathbb{Z}_N$ are parameterised by $a \in \mathbb{Z}_N$ with*

$$f_a : \mathbb{Z}_N \to \mathbb{Z}_N, \qquad f_a(n) := an.$$

The homomorphism f_a is a bijection (and hence an isomorphism) is a is relatively prime to N. That is, if $\gcd(a, N) = 1$.

We then have that

$$f_a \circ f_b = f_{a \cdot b}.$$

In the case that $N = 12$, we have that

$$\mathrm{Aut}(\mathbb{Z}_{12}) = \{f_1, f_5, f_7, f_{11}\}$$

and the composition table is given by

$\circ$	f_1	f_5	f_7	f_{11}
f_1	f_1	f_5	f_7	f_{11}
f_5	f_5	f_1	f_{11}	f_7
f_7	f_7	f_{11}	f_1	f_5
f_{11}	f_{11}	f_7	f_5	f_1

One of these entries would be calculated as

$$f_{11} \circ f_5 = f_{11 \cdot 5} = f_{55} = f_7.$$

The most difficult part of showing that $\mathrm{Aut}(G)$ is a group, is to show that it has inverses. This is covered by the following theorem.

Theorem 21. *Let G be a group, and $f \in \mathrm{Aut}(G)$. Then $f^{-1} \in \mathrm{Aut}(G)$.*

Proof. Let $g_1, g_2 \in G$, and define $x_1 := f^{-1}(g_1)$ and $x_2 := f^{-1}(g_2)$. We then have that $f(x_1) = g_1$ and $f(x_2) = g_2$. As f is a homomorphism we have that

$$g_1 \circ g_2 = f(x_1) \circ f(x_2) = f(x_1 \circ x_2).$$

Hence

$$f^{-1}(g_1 \circ g_2) = x_1 \circ x_2 = f^{-1}(g_1) \circ f^{-1}(g_2).$$

Thus f^{-1} is a homomorphism. As f is a bijection, we get that f^{-1} is a bijection and so f^{-1} is an isomorphism. □

Showing that $\mathrm{Aut}(G)$ is a group is now reasonably straightforward.

Theorem 22. *Let G be a group. Then $(\mathrm{Aut}(G), \circ)$ is a group.*

Proof. i) We define $\mathrm{id} : G \to G$ by $\mathrm{id}(g) = g$. As id is a bijection and homomorphism we have $\mathrm{id} \in \mathrm{Aut}(G)$. Let $f \in \mathrm{Aut}(G)$, and let $x \in G$. We have

$$(f \circ \mathrm{id})(x) = \mathrm{id}(f(x)) = f(x) = f(\mathrm{id}(x)) = (\mathrm{id} \circ f)(x).$$

Thus $f \circ \mathrm{id} = f = \mathrm{id} \circ f$.

ii) Let $f \in \mathrm{Aut(G)}$, then by the previous theorem we have $f^{-1} \in \mathrm{Aut(G)}$. To show $f^{-1} \circ f = \mathrm{id}$ we let $x \in G$. Then

$$(f^{-1} \circ f)(x) = f(f^{-1}(x)) = x = \mathrm{id}(x).$$

Thus $f^{-1} \circ f = \mathrm{id}$ as claimed.

iii) Let $f_1, f_2, f_3 \in \mathrm{Aut}(G)$, and let $x \in G$. Then

$$(f_1 \circ (f_2 \circ f_3))(x) = (f_2 \circ f_3)(f_1(x)) = f_3(f_2(f_1(x))),$$

and

$$((f_1 \circ f_2) \circ f_3)(x) = f_3((f_1 \circ f_2)(x)) = f_3(f_2(f_1(x))).$$

Thus $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$. □

We finish by defining a function from $G \to G$. We will eventually prove that this function is an automorphism of G.

Definition 15. *Let $g \in G$, and define a function $\phi_g : G \to G$ by*

$$\phi_g(h) = ghg^{-1}.$$

Lecture 17 (13-10-2023)

In this lecture we work out some example problems.

Example 14. *Compute the elements and the composition of the group* $\text{Aut}(\mathbb{Z}_{18})$.

Solution. *We have that the numbers* $\{0, 1, \cdots, 17\}$ *coprime to* 18 *are*

$$\{1, 5, 7, 11, 13, 17\}.$$

Thus

$$\text{Aut}(\mathbb{Z}_{18}) = \{f_1, f_5, f_7, f_{11}, f_{13}, f_{17}\}.$$

Using the rule $f_a \circ f_b = f_{ab}$ *we get the composition table*

$\circ$	f_1	f_5	f_7	f_{11}	f_{13}	f_{17}
f_1	f_1	f_5	f_7	f_{11}	f_{13}	f_{17}
f_5	f_5	f_7	f_{17}	f_1	f_{11}	f_{13}
f_7	f_7	f_{17}	f_{13}	f_5	f_1	f_{11}
f_{11}	f_{11}	f_1	f_5	f_{13}	f_{17}	f_7
f_{13}	f_{13}	f_{11}	f_1	f_{17}	f_7	f_5
f_{17}	f_{17}	f_{11}	f_1	f_{17}	f_7	f_5

Example 15. *Let* G *be a group, and let* $g \in G$. *We define* $\phi_g : G \to G$ *by*

$$\phi_g(h) = ghg^{-1}.$$

Show that $\phi_g \in \text{Aut}(G)$.

Solution. *Hom) Let* $h_1, h_2 \in G$. *Then*

$$\phi_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \phi_g(h_1)\phi_g(h_2).$$

Thus ϕ_g *is a homomorphism.*

Inj) Let $h \in \ker(\phi_g)$, *then* $ghg^{-1} = \phi_g(h) = e$. *Thus* $h = g^{-1}g = e$, *and so* ϕ_g *is injective.*

Sur) Let $y \in G$. *Then*

$$\phi_g(g^{-1}yg) = gg^{-1}ygg^{-1} = y.$$

Thus ϕ_g *is surjective.*

Example 16. *Show that*

$$H := \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{R}, ac \neq 0 \right\}$$

is a subgroup of $GL(2)$.

Solution. *As*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$$

we have that $H \neq \emptyset$.

Let

$$M_1 = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \in H \quad \textit{and} \quad M_2 = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \in H.$$

Then

$$M_1 \cdot M_2^{-1} = \frac{1}{a_2 c_2} \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} c_2 & -b_2 \\ 0 & a_2 \end{bmatrix} = \frac{1}{a_2 c_2} \begin{bmatrix} a_1 c_2 & -a_1 b_2 + b_1 a_2 \\ 0 & c_1 a_2 \end{bmatrix} \in H$$

Thus H *is a subgroup of* $GL(2)$.

Lecture 18 (16-10-2023)

In this lecture we begin to define the quotients of a group. These quotients can be thought of as identifying elements in a group together in way that results in a new group being produced.

Definition 16. *Let G be a group, and H a subgroup of G. We define*

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

Lets work some examples of this definition.

Example 17. *Let $G = D_6$, and $H_1 = \{e, r^2, r^4\}$ and $H_2 = \{e, s\}$. We then have*

$$D_6/H_1 = \{\{e, r^2, r^4\}, \{r, r^3, r^5\}, \{s, sr^2, sr^4\}, \{sr, sr^3, sr^5\}\}$$

and

$$D_6/H_2 = \{\{e, s\}, \{r, sr^5\}, \{r^2, sr^4\}, \{r^3, sr^3\}, \{r^4, sr^2\}, \{r^5, sr\}\}.$$

To define a composition on G/H we define the following.

Definition 17. *Let G be a group, and $X_1, X_2 \subseteq G$. We define*

$$X_1X_2 := \{x_1x_2 \mid x_1 \in X_1, x_2 \in X_2\}.$$

Let us compute some examples.

Example 18. *We have*

$$\{r, r^3, r^5\}\{s, sr^2, sr^4\} = \{sr^5, sr, sr^3\}$$

and

$$\{r, sr^5\}\{r^2, sr^4\} = \{r^3, sr^3, sr, r^5\}.$$

Note that in the first case the composition of two cosets is again a coset, while in the second case this is not true.

The following theorem shows that if H is a normal subgroup, then the composition of two cosets is again a coset.

Theorem 23. *Let G be a group, and H a normal subgroup. For all $g_1, g_2 \in G$ we have*

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Proof. $\subseteq$) Let $z \in (g_1H)(g_2H)$, then $z = x_1x_2$ for $x_1 \in g_1H$ and $x_2 \in g_2H$. Thus there exist $h + 1, h_2 \in H$ such that $x_1 = g_1h_1$ and $x_2 = g_2h_2$. Hence $z = g_1h_1g_2h_2$. As H is a normal subgroup, we have that $g_2^{-1}h_1g_2 = \hat{h}$ for some $\hat{h} \in H$. Hence $h_1g_2 = g_2\hat{h}$. Therefore

$$z = g_1h_1g_2h_2 = g_1g_2\hat{h}h_2 \in (g_1g_2)H$$

as $\hat{h}h_2 \in H$. Thus $(g_1H)(g_2H) \subseteq (g_1g_2)H$.

$\supseteq$) Let $z \in (g_1g_2)H$. Then $z = g_1g_2h$ for some $h \in h$. Thus

$$z = g_1eg_2h \in (g_1H)(g_2H)$$

as $e \in H$. Hence $(g_1g_2)H \subseteq (g_1H)(g_2H)$.

Together we get

$$(g_1H)(g_2H) = (g_1g_2)H$$

as claimed. □

This theorem allows us to quickly compute the composition of two cosets of a normal subgroup.

Example 19. *Let $G = D_6$ and $H = \{e, r^2, r^4\}$. We have the following compositions:*

$\circ$	H	rH	sH	srH
H	H	rH	sH	srH
rH	rH	H	srH	sH
sH	sH	srH	H	rH
srH	srH	sH	rH	H

Lecture 19 (18-10-2023)

The main goal of this lecture is to show that G/H is a group when H is normal.

Let us warm up by working an example.

Example 20. *Let $G = \mathbb{Z}_3 \times \mathbb{Z}_3$, and $H = \mathbb{Z}_3 \times \{0\}$. We then have*

$$G/H = \{H, \quad (0,1)H, \quad (0,2)H\}.$$

The composition we compute as

$\circ$	H	$(0,1)H$	$(0,2)H$
H	H	$(0,1)H$	$(0,2)H$
$(0,1)H$	$(0,1)H$	$(0,2)H$	H
$(0,2)H$	$(0,2)H$	H	$(0,1)H$

Lets now prove the main theorem.

Theorem 24. *Let G be a group, and H a normal subgroup. Then G/H is a group.*

Proof. First we show that composition is a function

$$G/H \times G/H \to G/H.$$

Let $X_1, X_2 \in G/H$, then there exist $g_1, g_2 \in G$ such that $X_1 = g_1H$ and $X_2 = g_2H$. Then

$$X_1X_2 = (g_1H)(g_2H) = (g_1g_2)H \in G/H.$$

Thus composition is indeed a function $G/H \times G/H \to G/H$.

We now show that the three conditions to be a group hold for our composition.

i) We claim that $H \in G/H$ is the identity. To see this let $X \in G/H$. Then $X = gH$ for some $g \in G$. Then

$$XH = (gH)(eH) = gH = X = gH = (eH)(gH) = HX.$$

Thus condition i) holds.

ii) Let $X \in G/H$, then there exists $g \in G$ such that $X = gH$. We claim that $X^{-1} = g^{-1}H$. We have

$$XX^{-1} = (gH)(g^{-1}H) = (gg^{-1})H = H.$$

Thus ii) holds.

iii) Let $X_1, X_2, X_3 \in G/H$, then there exist $g_1, g_2, g_3 \in G$ such that $X_1 = g_1H$, $X_2 = g_2H$, and $X_3 = g_3H$. Then

$$X_1(X_2X_3) = (g_1H)((g_2H)(g_3H)) = (g_1H)((g_2g_3)H) = (g_1g_2g_3)H,$$

and

$$(X_1X_2)X_3 = ((g_1H)(g_2H))(g_3H) = ((g_1g_2H))(g_3H) = (g_1g_2g_3)H.$$

Thus iii) holds and we are done. □

Note that in general we don't have that G/H is isomorphic to a subgroup of G. i.e. there is not an injective homomorphism $G/H \to G$. Instead we have that there is a surjective homomorphism from G onto G/H.

Definition 18. *Let G be a group, and H a normal subgroup. We define $\pi : G \to G/H$ by*

$$\pi(g) = gH.$$

Theorem 25. *Let G be a group, and H a normal subgroup. Then π is a surjective homomorphism.*

Proof. Hom) Let $g_1, g_2 \in G$, then

$$\pi(g_1)\pi(g_2) = (g_1H)(g_2H) = (g_1g_2)H = \pi(g_1g_2).$$

Thus π is a homomorphism.

Sur) Let $Y \in G/H$, then there exists $g \in G$ such that $Y = gH$. Hence

$$\pi(g) = gH = Y$$

and so π is surjective. □

Lecture 20 (20-10-2023)

In this lecture we work some example problems.

Exercise 14. *Determine the elements and composition of $D_6/\{e, r^3\}$.*

Solution. *We have that the six cosets of $H := \{e, r^3\}$ are*

$$\begin{aligned} H &= r^3H \\ rH &= r^4H \\ r^2H &= r^5H \\ sH &= sr^3H \\ srH &= sr^4H \\ sr^2H &= sr^5H. \end{aligned}$$

The composition we compute as

$\circ$	H	rH	r^2H	sH	srH	sr^2H
H	H	rH	r^2H	sH	srH	sr^2H
rH	rH	r^2H	H	srH	sr^2H	sH
r^2H	r^2H	H	rH	sr^2H	sH	srH
sH	sH	sr^2H	srH	H	r^2H	rH
srH	srH	sH	sr^2H	rH	H	r^2H
sr^2H	sr^2H	srH	sH	r^2H	rH	H

Exercise 15. *We are given a presentation for the quaternion group as follows:*

$$Q_8 := \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

a) List the elements of Q_8.

b) Show that $\{1, -1\}$ is a normal subgroup of Q_8.

c) Determine the structure of $Q_8/\{1, -1\}$.

Solution. *a) $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$.*

b) Let $g \in Q_8$, and note that $(-1)g = g(-1)$ for all $g \in Q_8$. We then have

$$g(1)g^{-1} = gg^{-1} = 1 \in \{1, -1\}$$

and

$$g(-1)g^{-1} = (-1)gg^{-1} = -1 \in \{1, -1\}$$

for all $g \in Q_8$. Thus $\{1, -1\}$ is normal.

c) The four cosets of $H := \{1, -1\}$ are

$$\begin{aligned} H &= -H \\ iH &= -iH \\ jH &= -jH \\ kH &= -kH. \end{aligned}$$

The composition we compute as

$\circ$	H	iH	jH	kH
H	H	iH	jH	kH
iH	iH	H	kH	jH
jH	jH	kH	H	iH
kH	kH	jH	iH	H

Lecture 21 (23-10-2023)

In this lecture we will begin to prove the first isomorphism theorem. The statement of this theorem is as follows.

Theorem 26. *Let G and H be groups, and $f : G \to H$ a homomorphism. Then*

$$G/\ker(f) \cong \operatorname{im}(f).$$

Before we prove this theorem, let us do an example to see its usefulness.

Example 21. *Let $G = GL(N)$ and consider the normal subgroup $\{M \in GL(N) \mid \det(M) = 1\}$. Intuition suggests that the quotient group should identify all matrices with the same determinant, and hence be isomorphic to $\mathbb{C} - \{0\}$. We can use the first isomorphism theorem to prove this. We have that $\det : GL(N) \to \mathbb{C} - \{0\}$ is a surjective homomorphism, and so Theorem 36 gives*

$$GL(N)/\ker(\det) = GL(N)/\{M \in GL(N) \mid \det(M) = 1\} \cong \mathbb{C} - \{0\}.$$

Before we can prove the first isomorphism theorem, we have to show that $\operatorname{im}(f)$ is a group.

Theorem 27. *Let G and H be groups, and $f : G \to H$ a homomorphism. Then $\operatorname{im}(f) := \{f(g) \mid g \in G\}$ is a subgroup of H.*

Proof. As $f(e_G) = e_H$, we have that $e_H \in \operatorname{im}(f)$ and so $\operatorname{im}(f) \neq \emptyset$.

Now let $f(g_1), f(g_2) \in \operatorname{im}(f)$. Then

$$f(g_1)f(g_2)^{-1} = f(g_1 g_2^{-1}) \in \operatorname{im}(f).$$

Hence $\operatorname{im}(f)$ is a subgroup of H. □

We are now set to prove the first isomorphism theorem.

Proof of Theorem 36. We define a function $F : G/\ker(f) \to \operatorname{im}(f)$ by $F(g\ker(f)) := f(g) \in \operatorname{im}(f)$. We need to show that F is well defined (i.e. doesn't depend on the choice of g used to represent the coset $g\ker(f)$), that F is a homomorphism, that F is injective, and that F is surjective.

Well Defined) Let g_1, g_2 such that $g_1\ker(f) = g_2\ker(f)$. Then $g_1 g_2^{-1} \in \ker(f)$ which implies that $f(g_1)f(g_2)^{-1} = e_H$. Hence $f(g_1) = f(g_2)$. Therefore

$$F(g_1\ker(f)) = f(g_1) = f(g_2) = F(g_2\ker(f))$$

and so F is a well defined function.

Hom) Let $g_1 \ker(f), g_2 \ker(f) \in G/\ker(f)$. Then

$$\begin{aligned} F((g_1 \ker(f))(g_2 \ker(f))) &= F((g_1 g_2) \ker(f)) \\ &= f(g_1 g_2) \\ &= f(g_1) f(g_2) \\ &= F((g_1 \ker(f))) F((g_2 \ker(f))). \end{aligned}$$

Thus F is a homomorphism.

Inj) Let $g \ker(f) \in \ker(F)$. Then $f(g) = F(g \ker(f)) = e_H$, and so $g \in \ker(f)$. Hence $g \ker(f) = \ker(f)$ and so $\ker(F) = \{\ker(f)\}$, which implies that F is injective.

Sur) Let $f(g) \in \operatorname{im}(f)$. Then

$$F(g \ker(f)) = f(g)$$

and so F is surjective.

□

Lecture 22 (25-10-2023)

In this lecture we introduce the centre of a group G. This will be the subset of G consisting of all elements of G which commute with all other elements.

Definition 19. *Let G be a group. We define*

$$Z(G) := \{h \in G \mid gh = hg \quad \textit{for all } g \in G\}.$$

Let us work a few examples to understand this definition.

Example 22. *Let $G = D_6$. Clearly we have $e \in Z(D_6)$ as $eg = g = ge$ for all $g \in G$. We also have $r^3 \in Z(D_6)$ as*

$$r^3 \circ r^i = r^{3+i} = r^i \circ r^3$$

and

$$r^3 \circ sr^i = r^3 sr^i = sr^{3+i} = sr^i \circ r^3.$$

Hence $r^3 \circ g = g \circ r^3$ for all $g \in D_6$.

We have $r \notin Z(D_6)$ as

$$r \circ s = sr^5 \neq s \circ r.$$

Similar reasoning gives that $r^2, r^4, r^5 \notin Z(D_6)$.

We have $s \notin Z(D_6)$ as

$$r \circ s = sr^5 \neq s \circ r.$$

Similar reasoning gives that $sr, sr^2, sr^3, sr^4, sr^5 \notin Z(D_6)$.

Thus

$$Z(D_6) = \{e, r^3\}.$$

Example 23. *Let $G = S_3$. As before we have that $e = () \in Z(S_3)$. We have*

$$(12) \circ (123) = (13) \neq (23) = (123) \circ (12).$$

This shows that $(12) \notin Z(S_3)$ and $(123) \notin Z(S_3)$. We also have

$$(23) \circ (132) = (13) \neq (12) = (132) \circ (23)$$

and so $(23) \notin Z(S_3)$ and $(132) \notin Z(S_3)$. Finally

$$(13) \circ (132) = (12) \neq (23) = (132) \circ (13)$$

and so $(13) \notin Z(S_3)$.

From these examples we can see that $Z(G)$ is a normal subgroup of G. We will now prove this holds in general.

Theorem 28. *Let G be a group. Then $Z(G)$ is a normal subgroup of G.*

Proof. As $eg = g = ge$ for all $g \in G$, we have that $e \in Z(G)$, and so $Z(G) \neq \emptyset$.

Let $h_1, h_2 \in Z(G)$, then $h_1 g = gh_1$ and $h_2 g = gh_2$ for all $g \in G$. Rearranging the last equation gives

$$gh_2^{-1} = h_2^{-1}g$$

for all $g \in G$. We then get that

$$gh_1h_2^{-1} = h_1gh_2^{-1} = h_1h_2^{-1}g$$

for all $g \in G$. Thus $h_1h_2^{-1} \in Z(G)$ and so $Z(G)$ is a subgroup of G.

To show $Z(G)$ is normal, let $k \in G$ and $h \in Z(G)$. Then $gh = hg$ for all $g \in G$. Thus $khk^{-1} = hkk^{-1} = h$, and so

$$g \circ (khk^{-1}) = gh = hg = (khk^{-1}) \circ g$$

for all $g \in G$. Thus $khk^{-1} \in Z(G)$ and so $Z(G)$ is normal.

□

Lecture 23 (27-10-2023)

In this lecture we work some practice problems.

Exercise 16. *Find all normal subgroups of S_3.*

Solution. *The subgroups of S_3 are*

$$\begin{aligned} &H_1 := \{()\} \\ &H_2 = S_3 \\ &H_3 = \{(), (123), (132)\} \\ &H_4 = \{(), (12)\} \\ &H_5 = \{(), (13)\} \\ &H_6 = \{(), (23)\} \end{aligned}$$

We have that H_1 and H_2 are normal immediately. We have that H_4 is not normal, as

$$(13)(12)(13)^{-1} = (13)(12)(13) = (23) \notin H_4.$$

The same logic gives H_5 and H_6 are not normal.

We have H_3 is normal as

$$\begin{aligned} (12)(123)(12) &= (132) \in H_3 \\ (23)(123)(23) &= (132) \in H_3 \\ (13)(123)(13) &= (132) \in H_3 \\ (12)(132)(12) &= (123) \in H_3 \\ (23)(132)(23) &= (123) \in H_3 \\ (13)(132)(13) &= (123) \in H_3. \end{aligned}$$

Thus the normal subgroups are H_1, H_2, and H_3.

Exercise 17. *Show that*

$$\mathbb{Z} \times \mathbb{Z} / \{(n, 3n) \mid n \in \mathbb{Z}\} \cong \mathbb{Z}.$$

Solution. *By the first isomorphism theorem, we can show the above by finding a surjective homomorphism $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ with $\ker(f) = \{(n, 3n) \mid n \in \mathbb{Z}\}$.*

We claim that $f(n, m) = 3n - m$ is such a homomorphism.

Hom) Let $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$. Then

$$f(a, b)f(c, d) = 3a-b+3c-d = 3(a+c)-(b+d) = f(a+c, b+d) = f((a, b)(c, d)).$$

Sur) Let $y \in \mathbb{Z}$. Then

$$f(0, -y) = y$$

so f is surjective.

Ker) Let $(n,m) \in \ker(f)$. Then $3n - m = f(n,m) = 0$, and so $m = 3n$. Thus $(n,m) = (n,3n)$, and so $\ker(f) = \{(n,3n) \mid n \in \mathbb{Z}\}$. The first isomorphism theorem then gives

$$\mathbb{Z} \times \mathbb{Z}/\{(n,3n)\} = \mathbb{Z} \times \mathbb{Z}/\ker(f) \cong \operatorname{im}(f) = \mathbb{Z}.$$

Exercise 18. *Find $Z(GL(2))$.*

Solution. *Let*

$$h = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(GL(2))$$

Then $hg = gh$ for all $g \in GL(2)$.

Consider $g = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL(2)$. Then

$$\begin{bmatrix} c & d \\ a & b \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & a \\ d & c \end{bmatrix}.$$

Thus $c = b$ and $a = d$.

Now consider Consider $g = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in GL(2)$. Then

$$\begin{bmatrix} -b & -a \\ a & b \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ b & a \end{bmatrix} = \begin{bmatrix} a & b \\ b & a \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & -a \\ a & -b \end{bmatrix}.$$

Thus $b = 0$, and so $h = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$. We then have for any $g = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in GL(2)$ that

$$gh = \begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} ax & ay \\ az & aw \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix} = hg.$$

Exercise 19. *Let $G = \mathbb{Z}_6 \times \mathbb{Z}_4$. Find a normal subgroup H such that $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Solution. *We define $f(a,b) := (a \mod 2, b \mod 2) : \mathbb{Z}_6 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$. This homomorphism is sujective as*

$$\begin{aligned} f(0,0) &= (0,0) \\ f(0,3) &= (0,1) \\ f(5,0) &= (1,0) \\ f(1,1) &= (1,1). \end{aligned}$$

The kernel of f consists of all elements $(a,b) \in \mathbb{Z}_6 \times \mathbb{Z}_4$ such that $a \mod 2 = 0$ and $b \mod 2 = 0$. This gives

$$\ker(f) = \{(0,0),(2,0),(4,0),(0,2),(2,2),(4,2)\}.$$

The first isomorphism theorem then gives

$$(\mathbb{Z}_6 \times \mathbb{Z}_4)/\{(0,0),(2,0),(4,0),(0,2),(2,2),(4,2)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Lecture 24 (30-10-2023)

In this lecture we introduce the semi-direct product of two groups G and H. A key ingredient for this construction will be a choice of homomorphism $\alpha : H \to \mathrm{Aut}(G)$. We will use the notation $\alpha_h := \alpha(h)$ to make our equations easier to read.

Definition 20. *Let G and H be groups, and $\alpha : H \to \mathrm{Aut}(G)$ a homomorphism. We define $G \overset{\alpha}{\rtimes} H$ as the set with elements*

$$\{(g,h) \mid g \in G \quad \textit{and} \quad h \in H\}$$

and with composition

$$(g_1, h_1) \circ (g_2, h_2) := (\alpha_{h_2}(g_1)g_2, h_1h_2).$$

Before we prove that $G \overset{\alpha}{\rtimes} H$ is a group, we will first work an example.

Example 24. *Let $G = \mathbb{Z}_3 = \{0,1,2\}$ and $H = \mathbb{Z}_2 = \{0,1\}$. We define $\alpha : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ by*

$$\begin{aligned} 0 &\to f_1 \\ 1 &\to f_2. \end{aligned}$$

Recall that f_1 is the identity automorphism of $\mathbb{Z}_3$, and f_2 exchanges the elements 1 and 2.

The elements of $\mathbb{Z}_3 \overset{\alpha}{\rtimes} \mathbb{Z}_2$ are

$$\{(0,0), (1,0), (2,0), (0,1), (1,1), (2,1)\}.$$

The composition table for these six elements is then

$\circ$	(0,0)	(1,0)	(2,0)	(0,1)	(1,1)	(2,1)
(0,0)	(0,0)	(1,0)	(2,0)	(0,1)	(1,1)	(2,1)
(1,0)	(1,0)	(2,0)	(0,0)	(1,1)	(2,1)	(0,1)
(2,0)	(2,0)	(0,0)	(1,0)	(2,1)	(0,1)	(1,1)
(0,1)	(0,1)	(2,1)	(1,1)	(0,0)	(2,0)	(1,0)
(1,1)	(1,1)	(0,1)	(2,1)	(1,0)	(0,0)	(2,0)
(2,1)	(2,1)	(1,1)	(0,1)	(2,0)	(1,0)	(0,0)

Inspection gives that this group is isomorphic to D_3 (or S_3).

We will now prove in general that $G \overset{\alpha}{\rtimes} H$ is a group.

Theorem 29. *Let G and H be groups, and $\alpha : H \to \mathrm{Aut}(G)$ a homomorphism. Then $G \overset{\alpha}{\rtimes} H$ is a group.*

Proof. i) We claim that (e_G, e_H) is the identity. To see this let $(g, h) \in G \overset{\alpha}{\rtimes} H$. Then

$$(e_G, e_H) \circ (g, h) = (\alpha_h(e_G) \circ g, h) = (e_G \circ g, h) = (g, h)$$

and

$$(g, h) \circ (e_G, e_H) = (\alpha_{e_H}(g) \circ e_G, h) = (\mathrm{id}_G(g), h) = (g, h).$$

Thus condition i) holds.

ii) Let $(g, h) \in G \overset{\alpha}{\rtimes} H$. We claim that

$$(g, h)^{-1} = (\alpha_{h^{-1}}(g^{-1}), h^{-1}).$$

To verify this claim we compute

$$\begin{aligned}
(g, h) \circ (\alpha_{h^{-1}}(g^{-1}), h^{-1}) &= (\alpha_{h^{-1}}(g) \circ \alpha_{h^{-1}}(g^{-1}), h \circ h^{-1}) \\
&= (\alpha_{h^{-1}}(g \circ g^{-1}), e_H) \\
&= (\alpha_{h^{-1}}(e_G), e_H) \\
&= (e_G, e_H).
\end{aligned}$$

Thus condition ii) holds.

iii) Let $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \overset{\alpha}{\rtimes} H$. Then

$$\begin{aligned}
(g_1, h_1) \circ ((g_2, h_2) \circ (g_3, h_3)) &= (g_1, h_1) \circ (\alpha_{h_3}(g_2)g_3, h_2h_3) \\
&= (\alpha_{h_2h_3}(g_1)\alpha_{h_3}(g_2)g_3, h_1h_2h_3) \\
&= ((\alpha_{h_2} \circ \alpha_{h_3})(g_1)\alpha_{h_3}(g_2)g_3, h_1h_2h_3).
\end{aligned}$$

On the other hand we have

$$\begin{aligned}
((g_1, h_1) \circ (g_2, h_2)) \circ (g_3, h_3) &= (\alpha_{h_2}(g_1)g_2, h_1h_2) \circ (g_3, h_3) \\
&= (\alpha_{h_3}(\alpha_{h_2}(g_1)g_2)g_3, h_1h_2h_3) \\
&= (\alpha_{h_3}(\alpha_{h_2}(g_1))\alpha_{h_3}(g_2)g_3, h_1h_2h_3) \\
&= ((\alpha_{h_2} \circ \alpha_{h_3})(g_1))\alpha_{h_3}(g_2)g_3, h_1h_2h_3).
\end{aligned}$$

These two terms are equal. Hence condition iii) holds, and so $G \overset{\alpha}{\rtimes} H$ is a group.

□

Lecture 25 (31-10-2023)

In this lecture we introduce two important theorems from group theory. We will not prove these theorems in this class. The first is to characterise semi-direct products.

Theorem 30. *Let G be a group, and H and K subgroups. If*

a) H is normal, and

b) $H \cap K = \{e\}$, and

c) $HK = G$,

then

$$G \cong H \overset{\alpha}{\rtimes} K$$

where $\alpha : K \to \mathrm{Aut}(H)$ is defined by

$$\alpha_k(h) = khk^{-1}.$$

Lets use this theorem in a few examples.

Example 25. *Let $G = D_N$. We have that $H = \{e, r, r^2, \cdots, r^{N-1}\} \cong \mathbb{Z}_N$ is a normal subgroup of G, and that $K = \{e, s\} \cong \mathbb{Z}_2$ is also a subgroup (but not a normal subgroup). We have that $H \cap K = \{e\}$, and that $HK = G$. Therefore the above theorem gives*

$$D_N \cong \mathbb{Z}_N \overset{\alpha}{\rtimes} \mathbb{Z}_2$$

where

$$\alpha_e(r^i) = er^ie = r^i$$
$$\alpha_s(r^i) = sr^is = r^{-i}$$

Example 26. *Let $G = \mathbb{Z}_4$. If we want to write G as a non-trivial semi-direct product, then we have to find subgroups H and K as in the above theorem. The subgroups of G are*

$$\{0\}$$
$$\{0, 2\}$$
$$\{0, 1, 2, 3\}$$

all of which are normal. However there is no way to pick H and K from these subgroups which give the conditions of the above theorem. Hence there is no way to write $\mathbb{Z}_4$ as a semi-direct product.

We will also state the classification of finite abelian groups. This theorem will be proved in Algebra 2.

Theorem 31. *Let G be a finite abelian group. Then*

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$$

where the p_i are primes which are not necessarily distinct, and the a_i are natural numbers.

Let us work some examples.

Example 27. *Let G be a an abelian group with order 4. We can write 4 as 2^2 or $2^1 \times 2^1$. Thus we have that either*

$$G \cong \mathbb{Z}_{2^2}$$

or

$$G \cong \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1}.$$

Example 28. *Let G be a an abelian group with order 6. The unique way to write 6 as a product of primes is $2^1 \times 3^1$. Hence*

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Example 29. *Let G be a an abelian group with order 8. We can write 8 as 2^3, or $2^2 \times 2^1$ or $2^1 \times 2^1 \times 2^1$. Thus we have that either*

$$G \cong \mathbb{Z}_{2^3}$$

or

$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2$$

or

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Example 30. *Let G be a an abelian group with order 36. We can write 36 as $2^2 \times 3^2$, or $2^1 \times 2^1 \times 3^2$, or $2^2 \times 3^1 \times 3^1$, or $2^1 \times 2^1 \times 3^1 \times 3^1$. Hence*

$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}$$

or

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$$

or

$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

or

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Lecture 26 (3-11-2023)

In this lecture we work out some practice problems.

Exercise 20. *Let $G = S_3$ and $H = \mathbb{Z}_2$. We define $\alpha : H \to \mathrm{Aut}(G)$ by $\alpha_0 = \mathrm{id}$, and α_1 the automorphism:*

$$\begin{aligned} () &\to () \\ (12) &\to (12) \\ (23) &\to (13) \\ (13) &\to (23) \\ (123) &\to (132) \\ (132) &\to (123) \end{aligned}$$

Find the smallest $n \in \mathbb{N}_{\geq 1}$ such that

$$((23), 1))^n = ((), 0).$$

Solution. *We have*

$$\begin{aligned} ((23), 1))^2 &= ((23), 1) \circ ((23), 1) = ((13)(23), 0) = ((123), 0) \\ ((23), 1))^3 &= ((123), 0) \circ ((23), 1) = ((132)(23), 1) = ((12), 1) \\ ((23), 1))^4 &= ((12), 1) \circ ((23), 1) = ((12)(23), 0) = ((132), 0) \\ ((23), 1))^5 &= ((132), 0) \circ ((23), 1) = ((123)(23), 1) = ((13), 1) \\ ((23), 1))^6 &= ((13), 1) \circ ((23), 1) = ((23)(23), 0) = ((), 0). \end{aligned}$$

Thus $n = 6$.

Exercise 21. *Find an injective homomorphism $\mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_9)$.*

Solution. *We have $\mathrm{Aut}(\mathbb{Z}_9) = \{f_1, f_2, f_4, f_5, f_7, f_8\}$. We must have $\alpha_0 = f_1$ as homomorphisms map identities to identities. If we try $\alpha_1 = f_4$, then we get $\alpha_2 = \alpha_{1+1} = \alpha_1 \circ \alpha_1 = f_4 \circ f_4 = f_{16} = f_7$. This gives an injective function α which we can directly check is a homomorphism.*

$$\begin{aligned} \alpha_1 \circ \alpha_1 &= f_4 \circ f_4 = f_{16} = f_7 = \alpha_{1+1} = \alpha_2 \\ \alpha_1 \circ \alpha_2 &= f_4 \circ f_7 = f_{28} = f_1 = \alpha_{1+2} = \alpha_0 \\ \alpha_2 \circ \alpha_1 &= f_7 \circ f_4 = f_{28} = f_1 = \alpha_{2+1} = \alpha_0 \\ \alpha_2 \circ \alpha_2 &= f_7 \circ f_7 = f_{49} = f_4 = \alpha_{2+2} = \alpha_1. \end{aligned}$$

Thus α is an injective homomorphism.

Exercise 22. *Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $H = \mathbb{Z}_2$. We define $\alpha : H \to \mathrm{Aut}(G)$ by*

$\alpha_0 = \mathrm{id}$ *and* α_1 *the automorphism:*

$$\begin{aligned}(0,0) &\to (0,0)\\ (0,1) &\to (1,0)\\ (1,0) &\to (0,1)\\ (1,1) &\to (1,1)\end{aligned}$$

We are given that $(\mathbb{Z}_2 \times \mathbb{Z}_2) \overset{\alpha}{\rtimes} \mathbb{Z}_2$ *is isomorphic to one of*

$$\mathbb{Z}_8, \quad \textit{or} \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \textit{or} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \textit{or} \quad D_4, \quad \textit{or} \quad Q_8.$$

Determine which one.

Solution. *Let's begin by counting the number of elements which are their own inverses in each of the 5 given groups.*

- *For* $\mathbb{Z}_8$ *there are two* $0, 4$.
- *For* $\mathbb{Z}_4 \times \mathbb{Z}_2$ *there are four* $(0,0), (1,0), (0,2), (1,2)$.
- *For* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ *every element is its own inverse, so there are eight.*
- *For* D_4 *there are six* $e, r^2, s, sr, sr^2, sr^3$.
- *For* Q_8 *there are two* $1, -1$.

We now compute the inverse of every element in $(\mathbb{Z}_2 \times \mathbb{Z}_2) \overset{\alpha}{\rtimes} \mathbb{Z}_2$. *We have*

$$\begin{aligned}((0,0),0)^{-1} &= ((0,0),0)\\ ((0,1),0)^{-1} &= ((0,1),0)\\ ((1,0),0)^{-1} &= ((1,0),0)\\ ((1,1),0)^{-1} &= ((1,1),0)\\ ((0,0),1)^{-1} &= ((0,0),1)\\ ((0,1),1)^{-1} &= ((1,0),1)\\ ((1,0),1)^{-1} &= ((0,1),1)\\ ((1,1),1)^{-1} &= ((1,1),1).\end{aligned}$$

We have that six of these are their own inverses. Thus $(\mathbb{Z}_2 \times \mathbb{Z}_2) \overset{\alpha}{\rtimes} \mathbb{Z}_2 \cong D_4$.

Lecture 27 (6-11-2023)

In this lecture we introduce the definition of a ring, study some examples, and prove a basic theorem.

Definition 21. *A ring is a triple* $(R, +, \times)$ *where* R *is a set, and* $+ : R \times R \to R$ *and* $\times : R \times R \to R$ *are functions satisfying:*

a) $a + (b + c) = (a + b) + c$ *for all* $a, b, c \in R$*,*

b) there exists $0 \in R$ *such that*

$$0 + a = a$$

for all $a \in R$*,*

c) for all $a \in R$*, there exists* $-a \in R$ *such that*

$$a + -a = 0,$$

d) $a + b = b + a$ *for all* $a, b \in R$*,*

e) $a \times (b \times c) = (a \times b) \times c$ *for all* $a, b, c \in R$*,*

f) there exists $1 \in R$ *such that*

$$1 \times a = a = a \times 1$$

for all $a \in R$*,*

g) $a \times (b + c) = a \times b + a \times c$ *for all* $a, b, c \in R$*,*

h) $(a + b) \times c = a \times c + b \times c$ *for all* $a, b, c \in R$*.*

The definition of a ring is a generalisation of properties of addition and multiplication on the integers $\mathbb{Z}$.

Some basic examples of rings are:

- $(\mathbb{Z}, +, \times)$,
- $(\mathbb{R}, +, \times)$,
- $(\mathbb{C}, +, \times)$.

A non-example is $(\mathbb{N}, +, \times)$, as we don't have additive inverses (condition c)).

A more complicated example is the following.

Example 31. *Let* $n \in \mathbb{N}$ *and define*

$$M_n(\mathbb{R}) := \{n \times n \textit{ matrices with entries in } \mathbb{R}\}.$$

We have that $(M_n(\mathbb{R}), +, \cdot)$ *is a ring where* $+$ *is the addition of matrices, and* $\cdot$ *is matrix multiplication.*

We could also define $M_n(\mathbb{Z})$ (matrices with integer entries), which is another example of a ring.

The last example of the day is the polynomial ring.

Example 32. *We define*

$$\mathbb{Z}[x] := \left\{ \sum_{i=0}^{n} c_i x^i : n \in \mathbb{N}_{\geq 0}, c_i \in \mathbb{Z} \right\}.$$

Some example elements of $\mathbb{Z}[x]$ *are*

- 1,
- $1 + 3x^2$,
- $3x^2 + 7x^5 + x^9$.

We then have that $\mathbb{Z}[x]$ *is a ring under addition and multiplication of polynomials.*

To end the lecture, we will prove a general theorem regarding rings.

Theorem 32. *Let* R *be a ring. Then*

$$0 \times a = 0 = a \times 0$$

for all $a \in R$.

Proof. We have that $0 + 0 = 0$. Thus

$$0 \times a = (0 + 0) \times a = 0 \times a + 0 \times a.$$

By adding $-(0 \times a)$ to both sides, we get

$$0 \times a + -(0 \times a) = 0 \times a + 0 \times a + -(0 \times a)$$

which implies that

$$0 = 0 \times a.$$

A near identical argument gives that

$$0 = a \times 0.$$

□

Lecture 28 (7-11-2023)

In this lecture we continue studying basic properties of rings.

Theorem 33. *Let R be a ring, and let $a, b \in R$. Then we have*

i) $a \times (-b) = (-a) \times b = -(a \times b)$

ii) $(-a) \times (-b) = a \times b$.

Proof. i) We have

$$a \times b + a \times (-b) = a \times (b - b) = a \times 0 = 0.$$

Hence

$$a \times (-b) = -(a \times b).$$

In a similar fashion we have

$$a \times b + (-a) \times b = (a - a) \times b = 0 \times b = 0.$$

Hence $(-a) \times b = -(a \times b)$.

ii) Using i) we have

$$(-a) \times (-b) = -(a \times (-b)) = -(-(a \times b)) = a \times b.$$

□

We now define the units of a ring.

Definition 22. *Let R be a ring. We define*

$$R^\times := \{r \in R : \textit{ there exists } w \in R \textit{ such that } r \times w = 1 = w \times r.\}$$

Some examples are:

- $\mathbb{Z}_4^\times = \{1, 3\}$,
- $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$,
- $\mathbb{Z}^\times = \{1, -1\}$,
- $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$,
- $\mathbb{Z}[\sqrt{2}] = \{\pm(1 + \sqrt{2})^n : n \in \mathbb{Z}\}$,
- $\mathbb{Z}[x] = \{1, -1\}$.

We can prove that $R^\times$ forms a group under multiplication.

Theorem 34. *Let R be a ring. We have that $(R^\times, \times)$ is a group.*

Proof. We first need to show that the multiplication of two units is again a unit. Let $r_1, r_2 \in R^\times$. Then there exists $w_1, w_2 \in R^\times$ such that $r_1 \times w_1 = w_1 \times r_1 = 1 = r_2 \times w_2 = w_2 \times r_2$. We then have

$$(r_1 \times r_2) \times (w_2 \times w_1) = r_1 \times r_2 \times w_2 \times w_1 = r_1 \times 1 \times w_1 = 1.$$

Hence $r_1 \times r_2 \in R^\times$ and $\times : R^\times \times R^\times \to R^\times$ is a function.

We now need to show the three conditions for a group.

i) We claim $e = 1$. To see this let $r \in R^\times$. Then

$$r \times 1 = r = 1 \times r.$$

Thus i) holds.

ii) Let $r \in R^x$, then there exists $w \in R^\times$ such that $r \times w = 1$. Thus $r^{-1} = w$ and ii) holds.

iii) Let $r_1, r_2, r_3 \in R^\times$. Then

$$r_1 \times (r_2 \times r_3) = (r_1 \times r_2) \times r_3$$

and so iii) holds. □

There are several additional properties a ring may have.

Definition 23. *Let R be a ring. If $a \times b = b \times a$ for all $a, b \in R$ we say that R is commutative.*

Definition 24. *Let R be a ring. If $R^\times = R - \{0\}$ we say that R is a division ring.*

Definition 25. *Let R be a ring, and $r \in R$. If there exists $s \in R$ such that $s \neq 0$ and $r \times s = 0$, we say that r is a zero divisor. If the only zero divisor of R is 0, then we say that R is a domain.*

Example 33. *We have that $\mathbb{Z}$ is a commutative ring, a domain, but not a division ring.*

Example 34. *We have that $\mathbb{Z}_5$ is a commutative ring, a domain, and a division ring.*

Example 35. *We have that $\mathbb{Z}[\sqrt{2}]$ is a commutative ring, a domain, and not a division ring.*

We end by introducing a new example.

Example 36. *We define*

$$\mathbb{H} := \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\}.$$

The addition is defined by

$$(a_1+b_1\mathbf{i}+c_1\mathbf{j}+d_1\mathbf{k})+(a_2+b_2\mathbf{i}+c_2\mathbf{j}+d_2\mathbf{k}) := (a_1+a_2)+(b_1+b_2)\mathbf{i}+(c_1+c_2)\mathbf{j}+(d_1+d_2)\mathbf{k}$$

and multiplication is defined by distributing and using the table

$\times$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	-1	$-\mathbf{k}$	$\mathbf{j}$
$\mathbf{j}$	$\mathbf{k}$	-1	$-\mathbf{i}$
$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{i}$	-1

The ring $\mathbb{H}$ is not commutative, but is a division ring, and a domain.

Lecture 29 (8-11-2023)

In this lecture we will work some example problems. By popular vote we will work on problems related to the examinable material.

Exercise 23. *Determine the elements of $Z(D_{12})$.*

Solution. *We have $Z(D_{12}) = \{e, r^6\}$.*

Exercise 24. *Determine the composition table for $D_4/\{e, r^2, sr, sr^3\}$.*

Solution. *We have that $H = \{e, r^2, sr, sr^3\}$ is one coset, and $rH = \{r, r^3, sr^2, s\}$ is the other coset. Thus the composition table is*

$\circ$	H	rH
H	H	rH
rH	rH	H

Exercise 25. *Show that*

$$\mathbb{Z}/\{3n : n \in \mathbb{Z}\} \cong \mathbb{Z}_3.$$

Solution. *We define a group homomorphism $f : \mathbb{Z} \to \mathbb{Z}_3$ by*

$$f(n) = n \mod 3.$$

We then have that $\ker(f) = \{3n : n \in \mathbb{Z}\}$ and so the first isomorphism theorem gives that

$$\mathbb{Z}/\{3n : n \in \mathbb{Z}\} \cong \operatorname{im}(f).$$

As $f(0) = 0$, $f(1) = 1$, $f(2) = 2$, we get that $\operatorname{im}(f) = \mathbb{Z}_3$ and so

$$\mathbb{Z}/\{3n : n \in \mathbb{Z}\} \cong \mathbb{Z}_3.$$

Exercise 26. *Find all g such that $g^2 = e$ in the group*

$$\mathbb{Z}_5 \overset{\alpha}{\rtimes} \mathbb{Z}_4$$

where

$$\begin{aligned} \alpha_0 &= f_1 \\ \alpha_1 &= f_2 \\ \alpha_2 &= f_4 \\ \alpha_3 &= f_3. \end{aligned}$$

Solution. *The elements are*

$$(0,0), \quad (0,2), \quad (1,2), \quad (2,2), \quad (3,2), \quad (4,2).$$

Exercise 27. *List all abelian groups with* 16 *elements.*

Solution. *These are*

$$\begin{aligned}
&\mathbb{Z}_{16}\\
&\mathbb{Z}_8 \times \mathbb{Z}_2\\
&\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2\\
&\mathbb{Z}_4 \times \mathbb{Z}_4\\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2
\end{aligned}$$

Exercise 28. *Give the composition table for* $\mathrm{Aut}(\mathbb{Z}_9)$*.*

Solution. *We have*

$\circ$	f_1	f_2	f_4	f_5	f_7	f_8
f_1	f_1	f_2	f_4	f_5	f_7	f_8
f_2	f_2	f_4	f_8	f_1	f_5	f_7
f_4	f_4	f_8	f_7	f_2	f_1	f_5
f_5	f_5	f_1	f_2	f_7	f_8	f_4
f_7	f_7	f_5	f_1	f_8	f_4	f_2
f_8	f_8	f_7	f_5	f_4	f_2	f_1

Lecture 30 (13-11-2023)

In this lecture we will have a review session for the upcoming exam.

Let's recall the key definitions.

The automorphism group of G is defined as:

Definition 26. *Let G be a group. We define*

$$\mathrm{Aut}(G) := \{f : G \to G \mid f \textit{ is an isomorphism } \}.$$

The semi-direct product is defined as:

Definition 27. *Let G and H be groups, and $\alpha : H \to \mathrm{Aut}(G)$ a homomorphism. We define $G \overset{\alpha}{\rtimes} H$ as the set with elements*

$$\{(g, h) \mid g \in G \quad \textit{and} \quad h \in H\}$$

and with composition

$$(g_1, h_1) \circ (g_2, h_2) := (\alpha_{h_2}(g_1)g_2, h_1h_2).$$

The centre of G is defined as:

Definition 28. *Let G be a group. We define*

$$Z(G) := \{h \in G \mid gh = hg \quad \textit{for all } g \in G\}.$$

The quotient group of G by H is defined as:

Definition 29. *Let G be a group, and H a subgroup of G. We define*

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

with composition

$$(g_1H) \circ (g_2H) = (g_1g_2)H.$$

We also recall some important theorems.

Theorem 35. *Let G be a finite abelian group. Then*

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$$

where the p_i are primes which are not necessarily distinct, and the a_i are natural numbers.

Theorem 36. *Let G and H be groups, and $f : G \to H$ a homomorphism. Then*

$$G/\ker(f) \cong \mathrm{im}(f).$$

Theorem 37. *Let G be a group, and H and K subgroups. If*

a) H is normal, and

b) $H \cap K = \{e\}$, and

c) $HK = G$,

then

$$G \cong H \overset{\alpha}{\rtimes} K$$

where $\alpha : K \to \mathrm{Aut}(H)$ is defined by

$$\alpha_k(h) = khk^{-1}.$$

Let us now look at some example questions.

Example 37. *Let*

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\}$$

Show that

$$G \cong H \overset{\alpha}{\rtimes} K$$

where

$$H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{R} \right\}$$

and

$$K = \left\{ \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix} : a, c \in \mathbb{R}, ac \neq 0 \right\}$$

for some $\alpha : K \to \mathrm{Aut}(H)$. You are given that H and K are subgroups of G.

Solution. *We will use the above theorem.*

a) To show H is normal , let $g = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in G$ and $h = \begin{bmatrix} 1 & b' \\ 0 & 1 \end{bmatrix} \in H$. Then

$$ghg^{-1} = \begin{bmatrix} 1 & \frac{ab'}{c} \\ 0 & 1 \end{bmatrix} \in H$$

Thus H is normal.

b) Let

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in H \cap K.$$

As $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in H$ we get $a = c = 1$, and as $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in K$ we get $b = 0$. Hence $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and so

$$H \cap K = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} = \{e\}.$$

c) Let $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in G$*. Then we have* $\begin{bmatrix} 1 & \frac{b}{c} \\ 0 & 1 \end{bmatrix} \in H$ *and* $\begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix} \in K$*. As*

$$\begin{bmatrix} 1 & \frac{b}{c} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}.$$

Thus $HK = G$*.*

As a), b) and c) are all satisfied, we get that

$$G \cong H \overset{\alpha}{\rtimes} K$$

for some $\alpha : K \to \mathrm{Aut}(H)$*.*

Example 38. *How many abelian groups are there with* $7^5 \times 3^3 \times 11^4$ *elements, up to isomorphism.?*

Solution. *There are 7 partitions of* 5*, 3 partitions of* 3 *and* 5 *partitions of* 4*. Thus there are*

$$7 \times 3 \times 5 = 105$$

abelian groups with $7^5 \times 3^3 \times 11^4$ *elements, up to isomorphism.*

Example 39. *Let* $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ *and* $H = \mathbb{Z}_3$*. We are given* $\alpha : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ *defined by* $\alpha_0 = \mathrm{id}$*, the automorphism* α_1 *defined by*

$$\begin{aligned} (0,0) &\mapsto (0,0) \\ (1,0) &\mapsto (0,1) \\ (0,1) &\mapsto (1,1) \\ (1,1) &\mapsto (1,0) \end{aligned}$$

and the automorphism α_2 *defined by*

$$\begin{aligned} (0,0) &\mapsto (0,0) \\ (1,0) &\mapsto (1,1) \\ (0,1) &\mapsto (1,0) \\ (1,1) &\mapsto (0,1) \end{aligned}$$

Find the elements of

$$Z((\mathbb{Z}_2 \times \mathbb{Z}_2) \overset{\alpha}{\rtimes} \mathbb{Z}_3).$$

Solution. *Note that*

$$((g_1, g_2), h_1) \circ ((0,0), h_2) = (\alpha_{h_2}((g_1, g_2)), h_1 + h_2)$$

while

$$((0,0), h_2) \circ ((g_1, g_2), h_1) = ((g_1, g_2), h_1 + h_2).$$

Thus if $(g_1, g_2) \neq (0,0)$ *we have that*

$$((g_1, g_2), h_1) \notin Z((\mathbb{Z}_2 \times \mathbb{Z}_2) \overset{\alpha}{\rtimes} \mathbb{Z}_3.$$

Further, if $h_2 \neq 0$*, we have that*

$$((0,0), h_2) \notin Z((\mathbb{Z}_2 \times \mathbb{Z}_2) \overset{\alpha}{\rtimes} \mathbb{Z}_3.$$

This leaves only the single element

$$\{((0,0),0)\} = Z((\mathbb{Z}_2 \times \mathbb{Z}_2) \overset{\alpha}{\rtimes} \mathbb{Z}_3$$

Example 40. *Use the first isomorphism theorem to show that*

$$\mathbb{Z}_{16}/\{0,4,8,12\} \cong \mathbb{Z}_4.$$

Solution. *We define a homomorphism* $f : \mathbb{Z}_{16} \to \mathbb{Z}_4$ *by*

$$f(n) = n \pmod 4.$$

We then have that

$$\ker(f) = \{0,4,8,12\}$$

and

$$\operatorname{im}(f) = \{0,1,2,3\}.$$

Thus the first isomorphism theorem gives

$$\mathbb{Z}_{16}/\{0,4,8,12\} \cong \mathbb{Z}_4.$$

Lecture 31 (17-11-2023)

In this lecture we work some practice problems related to rings.

Exercise 29. *Find the units and zero divisors of $\mathbb{Z}_8$. Further, give the composition table for the group of units.*

Solution. *We have that $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ as $1 \times 1 = 1$, $3 \times 3 = 1$, $5 \times 5 = 1$ and $7 \times 7 = 1$. The composition table is*

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

The zero divisors are

$$\{2, 4, 6\}.$$

Exercise 30. *Show that*

$$\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}] := \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$$

is a unit.

Solution. *We want to find $a, b, c, d \in \mathbb{Q}$ such that*

$$(\sqrt{2} + \sqrt{3}) \times (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = 1.$$

Expanding a grouping coefficients gives

$$(2b + 3c) + (a + 3d)\sqrt{2} + (a + 2d)\sqrt{3} + (b + c)\sqrt{6} = 1.$$

This gives the system of equations

$$\begin{aligned} 2b + 3c &= 1 \\ a + 3d &= 0 \\ a + 2d &= 0 \\ b + c &= 0. \end{aligned}$$

Solving this gives $a = 0, b = -1, c = 1, d = 0$. Thus

$$(\sqrt{2} + \sqrt{3}) \times (-\sqrt{2} + \sqrt{3}) = 1$$

and so $\sqrt{2} + \sqrt{3}$ is a unit in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Exercise 31. *Show that $\mathbb{Q}[\sqrt{3}]$ is a division ring.*

Solution. *Let $a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$ with either $a \neq 0$ or $b \neq 0$. We first aim to show that $a^2 - 3b^2 \neq 0$. For a contradiction, suppose that $a^2 - 3b^2 = 0$, then*

$$a^2 = 3b^2.$$

As either $a \neq 0$ or $b \neq 0$ we then have that both are non-zero. Thus we can divide to get

$$3 = \frac{a^2}{b^2}$$

which implies that

$$\sqrt{3} = \frac{a}{b} \in \mathbb{Q}$$

which is a contradiction. Thus $a^2 - 3b^2 \neq 0$.

We then have that

$$(a+b\sqrt{3})^-1 = \frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}.$$

As $\frac{a}{a^2-3b^2} \in \mathbb{Q}$ and $-\frac{b}{a^2-3b^2} \in \mathbb{Q}$ we have that $(a + b\sqrt{2})^-1 \in \mathbb{Q}[\sqrt{3}]$ and so $\mathbb{Q}[\sqrt{3}]$ is a division ring.

Lecture 32 (20-11-2023)

In this lecture we introduce subrings and ideals.

Definition 30. *Let R be a ring. We say $S \subseteq R$ is a subring if*

a) $0 \in S$ *and* $1 \in S$*,*

b) $-a \in S$ *for all* $a \in S$*,*

c) $a + b \in S$ *for all* $a, b \in S$*,*

d) $a \times b \in S$ *for all* $a, b \in S$*.*

These conditions ensure that S is a ring with operations and identities inherited from R.

Some examples are

- $\mathbb{Z} \subseteq \mathbb{Q}$,
- $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$,
- $\{a + 2b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}[\sqrt{2}]$,
- $\{\sum_{i=0}^{n} c_i x^{2i} \mid c_i \in \mathbb{Z}, n \in \mathbb{N}\} \subseteq \mathbb{Z}[x]$.

We have the following theorem which gives an easier way to prove something is a subring.

Theorem 38. *Let R be a ring, and $S \subseteq R$. Then S is a subring of R if and only if*

i) $1 \in S$*,*

ii) $a - b \in S$ *for all* $a, b \in S$*,*

iii) $a \times b \in S$ *for all* $a, b \in S$*.*

Proof. $\implies$) From a), b) and c) we have that $(S, +)$ is a subgroup of $(R, +)$. Thus $a - b \in S$ for all $a, b \in S$, giving ii). From a) we have $1 \in S$, so i) holds, and d) is exactly iii). Hence i), ii), and iii) hold.

$\impliedby$) From i) we have $1 \in S$ we have that $S \neq \emptyset$. Using ii) we then get that $(S, +)$ is a subgroup of $(R, +)$. Hence $0 \in S$, $-a \in S$ for all $a \in S$, and $a + b \in S$ for all $a, b \in S$. This gives a), b), and c). As iii) is exactly d) we have all of a), b), c), and d). Hence S is a subring. □

A related concept is that of an ideal of a ring.

Definition 31. *Let R be a ring. We say $I \subseteq R$ is a left ideal if*

a) $(I, +)$ *is a subgroup of* $(R, +)$*,*

b) $r \times x \in I$ *for all* $r \in R$ *and* $x \in I$*.*

Note that an ideal does not have to contain the element 1.

Some examples are:

1. $\{3n \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$,
2. $\{\sum_{i=2}^{n} c_i x^i \mid c_i \in \mathbb{Z}, n \in \mathbb{N}_{\geq 2}\} \subseteq \mathbb{Z}[x]$,
3. $\{0\} \subseteq \mathbb{Q}$,
4. $\mathbb{Z} \subseteq \mathbb{Z}$.

The ideals $\{0\} \subseteq R$ and $R \subseteq R$ are called the trivial ideals. In the case of division rings we have that there are no non-trivial ideals.

Theorem 39. *Let R be a division ring, and $I \subseteq R$ a left ideal. Then either $I = \{0\}$ or $I = R$.*

Proof. We either have $I = \{0\}$ or $I \neq \{0\}$. If $I = \{0\}$ we are done. If $I \neq \{0\}$ then there exists $0 \neq x \in I$. As R is a division ring, there exists $x^{-1} \in R$. Thus

$$1 = x^{-1} \times x \in I.$$

Now let $r \in R$. Then

$$r = r \times 1 \in I$$

and so $I = R$. □

Lecture 33 (27-11-2023)

In this lecture we define the notion of ring homomorphisms.

Definition 32. *Let R_1 and R_2 be rings. A ring homomorphism is a function $f : R_1 \to R_2$ such that*

a) $f(a + b) = f(a) + f(b)$ *for all* $a, b \in R_1$*,*

b) $f(a \times b) = f(a) \times f(b)$ *for all* $a, b \in R_1$*,*

c) $f(1_{R_1}) = 1_{R_2}$*.*

We have the following immediate result.

Theorem 40. *Let R_1 and R_2 be rings, and $f : R_1 \to R_2$ a ring homomorphism. Then*

i) $f(0_{R_1}) = 0_{R_2}$*,*

ii) $f(-a) = -f(a)$ *for all* $a \in R_1$*.*

Proof. We have that f is a group homomorphism from $(R_1, +)$ to $(R_2, +)$. The theorem then follows from Theorem 16. □

Let's now work an example.

Example 41. *Define* $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ *by*

$$f(a + b\sqrt{2}) = a - b\sqrt{2}.$$

We have that $f(1) = f(1 + 0\sqrt{2}) = 1$*. Thus c) holds.*

Let $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$*. We then have*

$$\begin{aligned} f(a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2}) &= f(a_1 + a_2 + (b_1 + b_2)\sqrt{2}) \\ &= a_1 + a_2 - (b_1 + b_2)\sqrt{2}) \\ &= a_1 - b_1\sqrt{2} + a_2 - b_2\sqrt{2} \\ &= f(a_1 + b_1\sqrt{2}) + f(a_2 + b_2\sqrt{2}), \end{aligned}$$

so a) holds, and

$$\begin{aligned} f((a_1 + b_1\sqrt{2}) \times (a_2 + b_2\sqrt{2})) &= f(a_1a_2 + 2b_1b_2 + (a_1b_2 + b_1a_2)\sqrt{2}) \\ &= a_1a_2 + 2b_1b_2 - (a_1b_2 + b_1a_2)\sqrt{2} \\ &= (a_1 - b_1\sqrt{2}) \times (a_2 - b_2\sqrt{2}) \\ &= f(a_1 - b_1\sqrt{2}) \times f(a_2 - b_2\sqrt{2}), \end{aligned}$$

so b) holds. Thus f is a ring homomorphism.

We now define the kernel of a ring homomorphism.

Definition 33. *Let R_1 and R_2 be rings, and $f : R_1 \to R_2$ a ring homomorphism. We define*
$$\ker(f) := \{r \in R \mid f(r) = 0_{R_2}\}.$$

We now prove that $\ker(f)$ is an ideal of R_1.

Theorem 41. *Let R_1 and R_2 be rings, and $f : R_1 \to R_2$ a ring homomorphism. Then $\ker(f)$ is a two-sided ideal of R_1.*

Proof. As $f(0_{R_1}) = 0_{R_2}$ we have that $0_{R_1} \in \ker(f)$ and so $\ker(f) \neq \emptyset$. Further, let $a, b \in \ker(f)$. Then $f(a) = 0_{R_2} = f(b)$, and so

$$f(a - b) = f(a) + f(-b) = f(a) - f(b) = 0_{R_2} - 0_{R_2} = 0_{R_2}.$$

Thus $a - b \in \ker(f)$ and so $\ker(f)$ is a subgroup of $(R, +)$.

Now let $r \in R_1$, and $a \in \ker(f)$. Then $f(a) = 0_{R_2}$ and so

$$f(a \times r) = f(a) \times f(r) = 0_{R_2} \times f(r) = 0_{R_2}$$

and

$$f(r \times a) = f(r) \times f(a) = f(r) \times 0_{R_2} = 0_{R_2}.$$

Thus $a \times r \in \ker(f)$ and $r \times a \in \ker(f)$, and so $\ker(f)$ is a two-sided ideal of R_1. □

Let us work another example.

Example 42. *Define $f : \mathbb{Z}[x] \to \mathbb{Z}$ by*

$$f\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} c_i.$$

We have $f(1) = f(1x^0) = 1$ so c) holds.

Let $p_1 = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$ and $p_2 = \sum_{i=0}^{n} d_i x^i \in \mathbb{Z}[x]$. Then

$$\begin{aligned} f(p_1 + p_2) &= f(\sum_{i=0}^{n}(c_i + d_i)x^i \\ &= \sum_{i=0}^{n}(c_i + d_i) \\ &= \sum_{i=0}^{n} c_i + \sum_{i=0}^{n} d_i \\ &= f(p_1) + f(p_2) \end{aligned}$$

so a) holds. We also have

$$\begin{aligned} f(p_1 \times p_2) &= f\left(\sum_{i=0}^{n}\sum_{j=0}^{n}(c_i \times d_i)x^{i+j}\right) \\ &= \sum_{i=0}^{n}\sum_{j=0}^{n}(c_i \times d_i) \\ &= \left(\sum_{i=0}^{n} c_i\right) \times \left(\sum_{j=0}^{n} d_j\right) \\ &= f(p_1) \times f(p_2) \end{aligned}$$

so b) holds. Thus f is a ring homomorphism.

We will prove one last theorem to end the lecture.

Theorem 42. *Let R be a commutative ring such that the only ideals are $I = \{0\}$ and $I = R$. Then R is a division ring.*

Proof. Let $a \in R$ be non-zero. Our goal is to find a multiplicative inverse for a. We define

$$\langle a \rangle := \{a \times r \mid r \in R\} \subseteq R.$$

We claim that $\langle a \rangle$ is an ideal of R. Indeed, we have that $\langle a \rangle$ is non-empty, as $a = a \times 1 \in \langle a \rangle$, and for $a \times r_1, a \times r_2 \in \langle a \rangle$ we have that

$$a \times r_1 - a \times r_2 = a \times (r_1 - r_2) \in \langle a \rangle.$$

Thus $\langle a \rangle$ is a subgroup of $(R, +)$.

Let $a \times r \in \langle a \rangle$ and $s \in R$. We then have

$$s \times (a \times r) = a \times (s \times r) \in \langle a \rangle.$$

Thus $\langle a \rangle$ is an ideal of R. As $a \neq 0$ and $a \in \langle a \rangle$, we can't have $\langle a \rangle = \{0\}$. Hence $\langle a \rangle = R$.

We have that $1 \in R$, and so $1 \in \langle a \rangle$. Thus there exists $r \in R$ such that $1 = a \times r$. Thus a has a multiplicative inverse.

As every non-zero element of R has a multiplicative inverse, we have that R is a division ring. □

Lecture 34 (29-11-2023)

In this lecture we introduce quotient rings. These are the analogues of quotient groups, and can be thought of as identifying elements in the ring with 0. The elements of the quotient ring will be additive cosets.

Definition 34. *Let R be a ring, and I a two-sided ideal. For $a \in R$ we define*

$$[a] := \{a + r \mid r \in I\}.$$

Note that I is a normal subgroup of $(R, +)$, and $[a]$ is the corresponding coset for a. This observation allows us to re-use several results on group cosets. The most important is the following.

Theorem 43. *Let R be a ring, I a two-sided ideal, and $a, b \in R$. Then $[a] = [b]$ if and only if $a - b \in I$.*

Proof. This is exactly Theorem 10 translated into ring notation. □

Let us work some quick examples.

Example 43. *Let $R = \mathbb{Z}_8$ and $I = \{0, 4\}$. We then have*

$$\begin{aligned}
[0] &= \{0, 4\} = [4] \\
[1] &= \{1, 5\} = [5] \\
[2] &= \{2, 6\} = [6] \\
[3] &= \{3, 7\} = [7].
\end{aligned}$$

Example 44. *Let $R = \mathbb{Z}[x]$ and $I = \{\sum_{i=2}^{n} c_i x^i \mid c_i \in \mathbb{Z}, n \in \mathbb{N}_{\geq 2}\}$. We have*

$$\begin{aligned}
[0] &= [x^2] = [5x^3 + 12x^{11}] \\
[1] &= [1 + x^2] = [1 + 2x^3 + 12x^4] \\
[x] &= [x + x^2] = [x + 4x^{12}]
\end{aligned}$$

The elements of the quotient ring will be the additive cosets.

Definition 35. *Let R be a ring, and I a two-sided ideal. We define*

$$R/I := \{[a] \mid a \in R\}.$$

To obtain a ring, we need to define an addition and a multiplication.

Definition 36. *Let R be a ring, I a two-sided ideal, and $a, b \in R$. We define*

$$\begin{aligned}
[a] + [b] &:= [a + b] \\
[a] \times [b] &:= [a \times b].
\end{aligned}$$

As these definitions depended on a choice of a and b in the coset, we need to make sure that the result doesn't change if we make a different choice.

Theorem 44. *Let R be a ring, I a two-sided ideal. Then the operations $+$ and $\times$ from Definition 36 are well-defined functions*

$$+ : R/I \times R/I \to R/I$$

and

$$\times : R/I \times R/I \to R/I.$$

Proof. We need to show that $+$ and $\times$ are well-defined operations on cosets. That is, we need to show that they do not depend on the choice of representative of the cosets. Let $a_1, a_2, b_1, b_2 \in R$ such that $[a_1] = [a_2]$ and $[b_1] = [b_2]$. Then we have that

$$a_1 - a_2 \in I \quad \text{and} \quad b_1 - b_2 \in I.$$

We then have

$$a_1 + b_1 - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I$$

Thus

$$[a_1] + [b_1] = [a_1 + b_1] = [a_2 + b_2] = [a_2] + [b_2].$$

Hence $+$ is a well defined function $+ : R/I \times R/I \to R/I$.

We also have

$$a_1 \times b_1 - a_2 \times b_2 = a_1 \times b_1 - a_1 \times b_2 + a_1 \times b_2 - a_2 \times b_2 = a_1 \times (b_1 - b_2) + (a_1 - a_2) \times b_2.$$

As I is a two-sided ideal, and $a_1 - a_2 \in I$ and $b_1 - b_2 \in I$ we have that $a_1 \times (b_1 - b_2) + (a_1 - a_2) \times b_2 \in I$. Hence $a_1 \times b_1 - a_2 \times b_2 \in I$ and so $[a_1 \times b_1] = [a_2 \times b_2]$. Thus

$$[a_1] \times [b_1] = [a_1 \times b_1] = [a_2 \times b_2] = [a_2] \times [b_2].$$

Hence $\times$ is a well defined function $\times : R/I \times R/I \to R/I$. □

We can now show that R/I is a ring.

Theorem 45. *Let R be a ring, I a two-sided ideal. Then R/I is a ring.*

Proof. We have to show that all 8 conditions for a ring are met. As $(R/I, +)$ is the quotient group of $(R, +)$ by the normal subgroup I, we have that a) associativity of $+$, b) additive identity, and c) additive inverses are satisfied.

d) Let $[a], [b] \in R/I$, then

$$[a] + [b] = [a + b] = [b + a] = [b] + [a].$$

Thus d) holds.

e)Let $[a], [b], [c] \in R/I$, then

$$[a] \times ([b] \times [c]) = [a] \times [b \times c] = [a \times b \times c] = [a \times b] \times [c] = ([a] \times [b]) \times [c].$$

Thus e) holds.

f) We claim [1] is the identity. Indeed let $[a] \in R/I$, then

$$[1] \times [a] = [a] = [a] \times [1].$$

Thus f) holds.

g/h) Let $[a], [b], [c] \in R/I$, then

$$[a] \times ([b] + [c]) = [a] \times [b + c] = [a \times (b + c)] = [a \times b + a \times c] = [a] \times [b] + [a] \times [c].$$

Hence g) holds. We also have

$$([a] + [b]) \times [c] = [a + b] \times c = [(a + b) \times c] = [a \times c + b \times c] = [a] \times [c] + [b] \times [c].$$

Thus h) holds.

All together we have that R/I is a ring. □

We end with a full example.

Example 45. *Let $R = \mathbb{Z}_9$ and $I = \{0, 3, 6\}$. Then*

$$R/I = \{[0], [1], [2]\}.$$

We have

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

and

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Lecture 35 (1-12-2023)

In this lecture we work through some practice problems.

Exercise 32. *Show that $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_7$ defined by*

$$f(a + b\sqrt{2}) = a + 3b \pmod 7$$

is a ring homomorphism.

Solution. *We have*

$$f(1) = f(1 + 0\sqrt{2}) = 1$$

so f preserves the identity.

Let $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then

$$\begin{aligned} f(a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2}) &= f(a_1 + a_2 + (b_1 + b_2)\sqrt{2}) \\ &= a_1 + a_2 + 3(b_1 + b_2) \\ &= a_1 + 3b_1 + a_2 + 3b_2 \\ &= f(a_1 + b_1\sqrt{2}) + f(a_2 + b_2\sqrt{2}). \end{aligned}$$

Thus f preserves addition. We also have

$$\begin{aligned} f(a_1 + b_1\sqrt{2}) \times f(a_2 + b_2\sqrt{2}) &= (a_1 + 3b_1)(a_2 + 3b_2) \\ &= a_1a_2 + 9b_1b_2 + 3(a_1b_2 + a_2b_1) \\ &= a_1a_2 + 2b_1b_2 + 3(a_1b_2 + a_2b_1) \\ &= f(a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2}) \\ &= f(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) \end{aligned}$$

and so f preserves multiplication.

Thus f is a ring homomorphism.

Exercise 33. *Give the multiplication tables for $\mathbb{Z}_6/\{0, 2, 4\}$ and $\mathbb{Z}_6/\{0, 3\}$.*

Solution. *For $I = \{0, 2, 4\}$ we have that*

$$\mathbb{Z}_6/\{0, 2, 4\} = \{[0], [1]\}.$$

The multiplication table we compute as

×	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

For $I = \{0, 3\}$ we have that

$$\mathbb{Z}_6/\{0, 3\} = \{[0], [1], [2]\}.$$

The multiplication table we compute as

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

The next two exercises are hard.

Exercise 34. *Find all zero divisors in*

$$\mathbb{Z}[x]/\left\{\sum_{i=3}^{n} c_i x^i \mid c_i \in \mathbb{Z}, n \in \mathbb{N}_{\geq 3}\right\}.$$

Solution. *The cosets for* $\left\{\sum_{i=3}^{n} c_i x^i \mid c_i \in \mathbb{Z}, n \in \mathbb{N}_{\geq 3}\right\}$ *are given by*

$$\left\{[a + bx + cx^2] \mid a, b, c \in \mathbb{Z}\right\}.$$

The multiplication we compute as

$$[a_1+b_1x+c_1x^2][a_1+b_1x+c_1x^2] = [a_1a_2+(a_1b_2+a_2b_1)x+(a_1c_2+a_2c_1+b_1b_2)x^2].$$

We can see that for any $b, c \in \mathbb{Z}$ *that*

$$[bx + cx^2][x^2] = [bx^3 + cx^4] = 0.$$

Thus all elements of the form $[bx + cx^2]$ *are zero-divisors.*

If we had any element of the form $[a_1 + b_1x + c_1x^2]$ *with* $a_1 \neq 0$ *such that*

$$[0] = [a_1+b_1x+c_1x^2][a_1+b_1x+c_1x^2] = [a_1a_2+(a_1b_2+a_2b_1)x+(a_1c_2+a_2c_1+b_1b_2)x^2]$$

then we get

$$\begin{aligned} a_1a_2 &= 0 \\ a_1b_2 + a_2b_1 &= 0 \\ a_1c_2 + a_2c_1 + b_1b_2 &= 0. \end{aligned}$$

Solving these equations gives that $a_2 = b_2 = c_2 = 0$*, and thus* $[a_1 + b_1x + c_1x^2]$ *is not a zero-divisor.*

Exercise 35. *Let* R *be a commutative ring such that there exists a prime* p *such that*

$$p \cdot r := \underbrace{r + r + \cdots + r}_{p \text{ times}} = 0.$$

Show that $f : R \to R$ *defined by* $f(r) = r^p$ *is a ring homomorphism.*

Solution. *The only non-trivial thing to check here is that f preserves addition. Let $a, b \in R$, then using the binomial expansion we get*

$$\begin{aligned} f(a+b) &= (a+b)^p \\ &= a^p + \binom{p}{1} \cdot a^{p-1} \times b + \binom{p}{2} \cdot a^{p-2} \times b^2 + \cdots \binom{p}{p-1} \cdot a^1 \times b^{p-1} + b^p. \end{aligned}$$

As p divides $\binom{p}{k}$, we have that $\binom{p}{k} \cdot r = 0$ for any $r \in R$. Thus $(a+b)^p = a^p + b^p = f(a) + f(b)$. Hence f preserves addition.

Lecture 36 (4-12-2023)

In this lecture we introduce and study fields.

Definition 37. *We say a ring R is a field if it is commutative, and it is a division ring.*

Let us study some examples and non-examples.

Example 46.

- $(\mathbb{R}, +, \times)$.
- $(\mathbb{Q}, +, \times)$.
- $\mathbb{Z}_5$ *(or $\mathbb{Z}_p$ for any prime p).*

Example 47. *Lets work out the multiplication table for $\mathbb{Z}_5$. We have*

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

As every non-zero element has an inverse, we have that $\mathbb{Z}_5$ is a field.

Example 48. *We have the following non-examples of fields.*

- $\mathbb{Z}$*, as $2 \in \mathbb{Z}$ does not have a multiplicative inverse.*
- $\mathbb{Z}_{16}$*, as 4 has no inverse.*
- $M_2(\mathbb{C})$*, is not commutative.*
- $\mathbb{Z}[x]$*, as $1 + x$ has no inverse.*

Example 49. *Let $R = \mathbb{Z}_{10}$ and let $I = \{0, 5\}$. Then*

$$R/I = \{[0], [1], [2], [3], [4]\}.$$

We have

$$\begin{aligned}
&[1] \times [1] = [1] \\
&[2] \times [3] = [6] = [1] \\
&[3] \times [2] = [6] = [1] \\
&[4] \times [4] = [16] = [6] = [1].
\end{aligned}$$

Thus R/I is a field.

Question: When is the quotient ring R/I a field.

Definition 38. *Let R be a commutative ring, and $I \subseteq R$ an ideal. We say I is a maximal ideal if for any ideal J such that $I \subset J \subseteq R$ we have that $J = R$.*

Example 50. *Consider $R = \mathbb{Z}_{20}$. The ideals for R are*

$$\begin{aligned}
I_1 &= \mathbb{Z}_{20}\\
I_2 &= \{0\}\\
I_3 &= \{0, 10\}\\
I_4 &= \{0, 5, 10, 15\}\\
I_5 &= \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}.
\end{aligned}$$

We have that I_1 is maximal. We have that I_2 is not maximal as $I_2 \subset I_4 \subseteq R$ but $I_4 \neq R$. We have that I_3 is not maximal as $I_3 \subset I_4 \subseteq R$ but $I_4 \neq R$. We have I_4 is a maximal ideal. We have that I_5 is a maximal ideal.

Example 51. *Consider*

$$I = \{2a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}[\sqrt{2}].$$

Let $\hat{I}$ be an ideal such that $I \subset \hat{I} \subseteq \mathbb{Z}[\sqrt{2}]$. Then we have that $\hat{I}$ contains an element of the form $2a+1+b\sqrt{2}$ for some $a, b \in \mathbb{Z}$. We also have that $\hat{I}$ contains the element $2a + b\sqrt{2}$. Then

$$1 = 2a + 1 + b\sqrt{2} - (2a + b\sqrt{2}) \in \hat{I}.$$

As $1 \in \hat{I}$ we get that $\hat{I} = \mathbb{Z}[\sqrt{2}]$. Hence I is a maximal ideal.

Theorem 46. *Let R be a commutative ring, and I a ideal. Then I is a maximal if and only if R/I is a field.*

Proof. Suppose I is a maximal ideal. We first show that R/I is commutative. Let $[a], [b] \in R/I$, then

$$[a] \times [b] = [a \times b] = [b \times a] = [b] \times [a].$$

To show that R/I is a division ring. Let $[a] \in R/I$ such that $[a] \neq [0]$. Then $a \notin I$. We define

$$\hat{I} := \{r \times a + b \mid r \in R \text{ and } b \in I\} \subseteq R.$$

We also have that $I \subset \hat{I}$. We claim that $\hat{I}$ is an ideal in R.

We have that $\hat{I}$ is non-empty as

$$0 = 0 \times a + 0 \in \hat{I}.$$

Let $r_1 \times a + b_1, r_2 \times a + b_2 \in \hat{I}$. Then

$$r_1 \times a + b_1 - r_2 \times a - b_2 = (r_1 - r_2) \times a + (b_1 - b_2) \in \hat{I}$$

as $b_1 - b_2 \in I$. Thus $\hat{I}$ is a subgroup of $(R, +)$.

Let $r_1 \times a + b \in \hat{I}$, and $r_2 \in R$. Then

$$r_2 \times (r_1 \times a + b) = r_2 \times r_1 \times a + r_2 \times b \in \hat{I}$$

as $r_2 \times b \in I$. Thus is $\hat{I}$ is an ideal.

As I is maximal, we have that $\hat{I} = R$. We know that $1 \in R = \hat{I}$. Thus $1 = r \times a + b$ for some $r \in R$ and some $b \in I$. Then we have

$$\begin{aligned}
[a] \times [r] &= [a \times r] \\
&= [r \times a] \\
&= [1 - b] \\
&= [1] - [b] \\
&= [1] - [0] \\
&= [1].
\end{aligned}$$

Thus $[a]$ has a multiplicative inverse, thus R/I is a division ring.

Suppose that R/I is a field. Let J be an ideal such that $I \subset J \subseteq R$. Our goal is to show that $J = R$. Let $a \in J - I$, then $a \notin I$, and so $[a] \neq [0]$. Thus there exists $[b] \in R/I$ such that $[a] \times [b] = [1]$. As $[1] = [a] \times [b] = [a \times b]$. Hence $a \times b - 1 \in I \subset J$. As $a \in J$ and $b \in R$ we get $a \times b \in J$. We then have

$$1 = a \times b - (a \times b - 1) \in J.$$

As $1 \in J$, and so $J = R$. Hence I is maximal. □

Lecture 37 (6-12-2023)

Recall that R is a domain if it has no zero-divisors.

Example 52. *The following are domains*

- $\mathbb{Z}$,
- $\mathbb{R}$,
- $\mathbb{Z}[x]$.

We have the following non-examples.

- $M_2(\mathbb{R})$,
- $\mathbb{Z}[x]/\langle x^2 \rangle$

The question we want to answer is the following: When is R/I a domain?

Definition 39. *Let R be a ring, and $I \subseteq R$ an ideal. We say I is a prime ideal if for all $a, b \in R$ we have*

$$a \times b \in I \implies a \in I \text{ or } b \in I.$$

Let us look at some examples. Before we do this, let us recall a basic fact.

Theorem 47. *Let p be a prime number and let $a, b \in \mathbb{Z}$. Then*

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Example 53. *Let $R = \mathbb{Z}$ and define*

$$I = \{3n \mid n \in \mathbb{Z}\}.$$

Let $a, b \in \mathbb{Z}$ such that $ab \in I$. Thus there exists $n \in \mathbb{Z}$ such that $ab = 3n$. Hence $3 \mid ab$, and so $3 \mid a$ or $3 \mid b$. Therefore $a \in I$ or $b \in I$. Thus I is a prime ideal.

We will also study a non-example.

Example 54. *Let $R = \mathbb{Z}$ and define*

$$I = \{4n \mid n \in \mathbb{Z}\}.$$

We have that $4 \in I$. As $4 = 2 \times 2$, and $2 \notin I$, we have that I is not a prime ideal.

Let us a prove a general theorem generalising these examples.

Theorem 48. *Let $m \in \mathbb{Z}_{\geq 1}$ and define*

$$I_m := \{mn \mid n \in \mathbb{Z}\}.$$

Then I_m is a prime ideal if and only if m is prime.

Proof. Assume that m is prime. Let $a, b \in \mathbb{Z}$ such that $ab \in I_m$. Thus there exists $n \in \mathbb{Z}$ such that $ab = mn$. Hence $m \mid ab$, and so $m \mid a$ or $m \mid b$. Thus $a \in I_m$ or $b \in I_m$. Therefore I_m is a prime ideal.

Assume that m is not prime. Thus $m = m_1 \times m_2$ for $m_1, m_2 \in \mathbb{Z}_{\geq 2}$. We have that $m_1 \times m_2 = m \in I_m$.

For a contradiction assume that $m_1 \in I_m$. Then $m_1 = mn$ for some $n \in \mathbb{Z}$. This implies that $m_1 = m_1 \times m_2 \times n$, and so

$$1 = m_2 \times n.$$

Thus $m_2 = 1$ which contradicts $m_2 \geq 2$. Thus $m_1 \notin I_m$.

The same argument shows that $m_2 \notin I_m$, and so I_m is not a prime ideal. □

We can now prove our main theorem.

Theorem 49. *Let R be a commutative ring, and $I \subseteq R$ an ideal. Then R/I is a domain if and only if I is a prime ideal.*

Proof. Assume that R/I is a domain. Let $a, b \in R$ such that $a \times b \in I$. Then we have

$$[a] \times [b] = [a \times b] = [0].$$

As R/I is a domain, we have either $[a] = [0]$ or $[b] = [0]$. Thus $a \in I$ or $b \in I$, and so I is a prime ideal.

Assume I is a prime ideal. Let $[a] \in R/I$ be a zero-divisor. Thus there exists $[b] \in R/I$ such that $[b] \neq [0]$ and such that

$$[a \times b] = [a] \times [b] = [0].$$

Therefore $a \times b \in I$. Thus either $a \in I$ or $b \in I$, which implies either $[a] = [0]$ or $[b] = [0]$. We know $[b] \neq [0]$, so $[a] = [0]$. Thus the only zero-divisor in R/I is $[0]$, and so R/I is domain. □

Lecture 38 (8-12-2023)

Exercise 36. *Let $R = \mathbb{Z}[x]$ and let*

$$I := \left\{ \sum_{i=2}^{n} c_i x^i \mid c_i \in \mathbb{Z}, n \in \mathbb{N}_{\geq 2} \right\} \subset \mathbb{Z}[x].$$

Is I maximal, and is I prime?

Proof. Let us consider R/I. We have

$$R/I = \{[a + bx] \mid a, b \in \mathbb{Z}\}.$$

Now lets consider the element $[x] \in R/I$. We have

$$[x] \times [x] = [x^2] = [0].$$

Thus $[x]$ is a zero-divisor in R/I and so R/I is not a domain. Hence I is not prime.

For a contradiction, assume there exists $[a + bx] \in R/I$ such that

$$[x] \times [a + bx] = [1].$$

This gives us

$$[ax] = [ax + bx^2] = [1].$$

Hence $ax - 1 \in I$, but $ax - 1 \notin I$, and so $[x]$ has no multiplicative inverse. Hence R/I is not a field, and so I is not maximal. □

Exercise 37. *Lets define*

$$I := \{2a + 2b\sqrt{3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{Z}[\sqrt{3}].$$

Show that I is not a maximal ideal.

Proof. We have that

$$\begin{aligned}
[0] &= \{2a + 2b\sqrt{3} \mid a, b \in \mathbb{Z}\} \\
[1] &= \{2a + 1 + 2b\sqrt{3} \mid a, b \in \mathbb{Z}\} \\
[\sqrt{3}] &= \{2a + (2b + 1)\sqrt{3} \mid a, b \in \mathbb{Z}\} \\
[1 + \sqrt{3}] &= \{2a + 1 + (2b + 1)\sqrt{3} \mid a, b \in \mathbb{Z}\}
\end{aligned}$$

Thus $R/I = \{[0], [1], [\sqrt{3}], [1 + \sqrt{3}]\}$. We compute

$\times$	$[0]$	$[1]$	$[\sqrt{3}]$	$[1+\sqrt{3}]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[\sqrt{3}]$	$[1+\sqrt{3}]$
$[\sqrt{3}]$	$[0]$	$[\sqrt{3}]$	$[1]$	$[1+\sqrt{3}]$
$[1+\sqrt{3}]$	$[0]$	$[1+\sqrt{3}]$	$[1+\sqrt{3}]$	$[0]$

We can see that R/I is not a field, hence I is not maximal. □

Exercise 38. *Find all maximal ideals in $\mathbb{Z}_{16}$.*

Proof. We have that the ideals in $\mathbb{Z}_{16}$ are

$$\begin{aligned} I_1 &= \mathbb{Z}_{16} \\ I_2 &= \{0\} \\ I_3 &= \{0, 8\} \\ I_4 &= \{0, 4, 8, 12\} \\ I_5 &= \{0, 2, 4, 6, 8, 10, 12, 14\}. \end{aligned}$$

We can see that the maximal ideals are I_1 and I_5. □