MAT1100 - Grublegruppe
Extra Problems 9

Jørgen O. Lye

More Group Theory

This note is going to define something called quotient groups and look at further examples of groups. Before we can define quotient groups, we need to look at something called equivalence relations.

Equivalence Relations

The concept of equivalence relations is both useful and widespread in mathematics and physics. An equivalence relation $\sim$ on a set X is such that

- $x \sim y \implies y \sim x$.
- $x \sim x$.
- $x \sim y$ and $y \sim z \implies x \sim z$.

These are called "symmetry", "reflexivity", and "transitivity", respectively. The first example the reader should have no problem verifying is that $=$ is an equivalence relation. Note that $\leq$, $\geq$ $<$ and $>$ are *not* equivalence relations.

Example

A slightly more non-trivial relation which is very useful is the following example. Let X be some set and write $X = A \bigcup B$ for **disjoint** subset A and B. We can define a relation on X by saying $x \sim y$ if x and y are both in A or both in B. Show this this is indeed an equivalence relation.

Example

Consider the set $\mathbf{Z}$ with addition. Pick some number $p \in \mathbf{Z}$. Define $x \sim y$ if and only if $x - y = n \cdot p$ for some $n \in \mathbf{Z}$. Show that this is an equivalence relation.

Quotients

Let X be some set with an equivalence relation $\sim$ defined on it. Show that this gives rise to a partition $X = \bigcup U_\alpha$ into disjoint sets where $x, y \in U_\alpha \iff x \sim y$. We call the sets U_α equivalence classes.

We can now define the quotient of X written $X/\sim$. This is the set of equivalence classes, U_α. I.e. we're going to think about entire equivalence classes as points. Some examples should help here.

Examples

Let X be any set and define $\sim$ to be simply $=$. Argue that $X/\sim$ is in 1-to-1 correspondence with X.

Now define a different relation on X to be $x \sim y$ for any x, y. Argue why this is an equivalence relation. Then argue that $X/\sim$ consists of a single point, i.e. that there is a single equivalence class.

Example

Recall that last time we had the group $\mathbf{Z}/(p\mathbf{Z}) = \{0, 1, \cdots p-1\}$ with addition modulo p. Argue that if you define the equivalence relation $\sim$ on $\mathbf{Z}$ as above, then $\mathbf{Z}/\sim$ can be identified with $\mathbf{Z}/(p\mathbf{Z})$.

Quotient groups

Let G be a group and let $H \subset G$ be a group. H is then called a **subgroup** of G. Examples include $\mathbf{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Notice that there are always at least two subgroups of a group; $H = \{e\}$ and $H = G$. These are called trivial subgroups, and aren't really that interesting. There is more you can do with subgroups on their own, but we're going to study quotients.

The intuition of the group G/H, the "quotient of G by H", is that it is elements of G where things in H are set to e. Here is a more formal definition. Assume H is a **normal** subgroup of G, which means that $g * h * g^{-1} \in H$ for all $g \in G$ and $h \in H$. I am not saying $gh = hg$, but if this holds than H is normal. In particular, any subgroup of an abelian group is normal. As a set, define $G/H = \{g * H | g \in G\}$, where $g * H$ means $\{g * h | h \in H\}$. Define a group operation on this set by

$$(g_1 * H) * (g_2 * H) = (g_1 * g_2) * H$$

This is well-defined, since H is normal:

$$(g_1 * H) * (g_2 * H) = g_1 * (H * g_2) * H = g_1 * (g_2 * H) * H = (g_1 * g_2) * H$$

Notice that $G/G \cong \{e\}$ and $G/\{e\} \cong G$. More examples are definitively in order:

Example

Pick some $p \in \mathbf{Z}$ and let $p\mathbf{Z}$ be the set $\{p * n | n \in \mathbf{Z}\}$. This is a subgroup of $\mathbf{Z}$. Argue that the group $\mathbf{Z}/(p\mathbf{Z})$ (as a quotient group) coincides with what I defined last time, i.e. addition modulo p. This is a good example of what I meant by G/H is G where everything in H is 0.

Argue also that $\mathbf{Z}/(1\mathbf{Z}) \cong \{0\}$ and $\mathbf{Z}/(0\mathbf{Z}) \cong \mathbf{Z}$. This is often written briefly as $\mathbf{Z}/(1) = 0$, $\mathbf{Z}/0 = \mathbf{Z}$. I know this might look a bit strange the first time.

Example

Similarly, let $2\pi i\mathbf{Z} = \{2\pi i \cdot n | n \in \mathbf{Z}\}$. Argue that

$$\mathbb{C}/(2\pi i\mathbf{Z}) \cong \{z \in \mathbb{C} | 0 \leq \mathrm{Im}(z) < 2\pi i\}$$

where addition is modulo $2\pi i$ in the imaginary part. What does the above set look like in the plane?

Example

We saw last time that we could view $\mathbf{Z}/(p\mathbf{Z}) \cong C_p$ as the set of unit p'th roots in the complex plane. This is a subgroup of $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Argue that

$$\mathbb{C}^*/C_p \cong \{z = re^{i\theta} | r > 0,\ 0 \leq \theta < \frac{2\pi}{p}\}$$

What does this set look like in the complex plane?

Kernels

Recall last time that we argued

$$\mathbb{R} \cong \mathbb{R}^+$$

where the group homomorphism was $\exp(x)$. We also saw that

$$\exp : \mathbb{C} \to \mathbb{C}^*$$

was a group homomorphism. You might also have convinced yourself that it was surjective but not injective. We're going to fix that now.

Problem

If $\phi : H \to G$ is any group homomorphism, denote by $\ker(\phi) = \{h \in H | \phi(h) = e_G\}$. This is called the kernel of ϕ. Show that it is a subgroup of H.

Show that a homomorphism is injective if and only if $\ker(\phi) = \{e_H\}$.

Example

We saw that $\exp : \mathbb{R} \to \mathbb{R}^+$ had $\ker(\exp) = \{0\}$, i.e. it was injective. We also saw that for $\exp : \mathbb{C} \to \mathbb{C}^*$ we had $\ker(\exp) = 2\pi i\mathbf{Z}$. Argue why exp is injective when considered as a function

$$\exp : \mathbb{C}/(2\pi i\mathbf{Z}) \to \mathbb{C}^*$$

while remaining surjective. What I claim is precisely that as groups,

$$\mathbb{C}/(2\pi i\mathbf{Z}) \cong \mathbb{C}^*$$

Problem

The unit circle $\mathbb{S}^1 \subset \mathbb{C}^*$ is a multiplicative group $e^{i\theta_1}e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$. Argue that

$$\mathbb{S}^1 \cong \mathbb{R}/(2\pi\mathbf{Z})$$

and

$$\mathbb{S}^1 \cong \mathbb{C}^*/\mathbb{R}^+$$