Monday: Isomorphisms and homomorphisms

We have already used the word "isomorphism" in Section 5.4 of the textbook, when we said that two partially ordered sets $(A, \preceq_A)$ and $(B, \preceq_B)$ are *order-isomorphic* if there is a bijection $f : A \to B$ such that for every $x, y \in A$,

$$f(x) \preceq_B f(y) \text{ if and only if } x \preceq_A y.$$

We can think of this as meaning that B is really just a "re-labelled" version of A, with exactly the same structure.

We can do the same thing for groups. In this case, the structure we have is not an order relation but a binary operation, but the idea—that the isomorphism should preserve the structure—is exactly the same.

Definition. *Let $(G, *)$ and $(H, \diamond)$ be groups. A* homorphism *from G to H is a function $f : G \to H$ such that for all $x, y \in G$,*

$$f(x * y) = f(x) \diamond f(y).$$

An isomorphism *from G to H is a homomorphism from G to H which is also a bijection. If there is such an isomorphism, we say that G and H are* isomorphic, *written $G \approx H$.*

Example 1. *Let $n \in \mathbb{N}$. The function $f : \mathbb{Z} \to \mathbb{Z}_n$ given by $f(x) = \overline{x}$ is a homomorphism, since for every $x, y \in \mathbb{Z}$ we have $\overline{x+y} = \overline{x} + \overline{y}$. However, it is not an isomorphism because it is not 1–1: we have $0 \neq n$ but $\overline{0} = \overline{n}$.*

Example 2. *Let $U(10) = \{1, 3, 7, 9\}$. We define an operation $\diamond$ by declaring that, for $x, y \in U(10)$, $x \diamond y$ is the remainder modulo 10 of $x \cdot y$. Let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, and define an operation $*$ on $\mathbb{Z}_4$ by declaring that $x * y = x +_4 y$. So we have the Cayley tables*

$\diamond$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Then the function $f : \mathbb{Z}_4 \to U(10)$ given by $f(0) = 1$, $f(1) = 3$, $f(2) = 9$, $f(3) = 7$ is an isomorphism.

Proposition 3. *Let G and H be groups with identity elements e_G and e_H respectively, and let $f : G \to H$ be a homorphism. Then $f(e_G) = e_H$.*

Proposition 4. *Let G and H be groups with identity elements e_G and e_H respectively, and let $f : G \to H$ be an isomorphism. Then, for every $x \in G$, we have*

$$f(x) \diamond f(y) = e_H \text{ if and only if } x * y = e_G.$$

Exercise 5. *Let G be the group given by the group table*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Show that G is not *isomorphic to $\mathbb{Z}_4$.*

Tuesday: Subgroups

From now on we will use a convenient convention: we will omit the group operation symbol, just as when we are multiplying numbers we omit the $\cdot$. So for example we will write gh instead of $g * h$. We also write g^2 for gg, g^3 for ggg, g^{-3} for $(g^{-1})^3$ and so on.

Definition. *A* subgroup *of a group $(G, *)$ is a subset H of G such that $*$ is a group operation on H.*

Example 6. *$\mathbb{Z}$ is a subgroup of the group $(\mathbb{R}, +)$.*

Example 7. *The set $H = \{R_0, R_{90}, R_{180}, R_{270}\}$ is a subgroup of D_4.*

Proposition 8. *A subset H of a group G is a subgroup of G if and only if*

1. *$e \in H$ (where e is the identity element of G);*
2. *for any $x, y \in H$, $xy \in H$; and*
3. *for any $x \in H$, $x^{-1} \in H$.*

Proposition 9. *A subset H of a group G is a subgroup of G if and only if $H \neq \emptyset$ and, for every $x, y \in H$, $xy^{-1} \in H$.*

Our goal for this section will be to prove *Lagrange's Theorem.* This is the statement that if G is a finite group and H is a subgroup of G then the number of elements of G is a multiple of the number of elements of H.

To prove this, we will show that we can use the subgroup H to form a partition of G. The number of elements in each set in the partition will be the same as the number of elements in H. Thus the number of elements in G is equal to the number of elements in H times the number of sets in the partition. And that's all there is to it! Of course, we have to check the details.

Definition. *Let H be a subgroup of a group G, and let $a \in G$. We define the* left coset of H in G containing a, *written aH, by*

$$aH = \{\, ah : h \in H \,\}.$$

Lemma 10. *Let H be a subgroup of G and let $a, b \in G$. If $aH \cap bH \neq \emptyset$ then $aH = bH$.*

Lemma 11. *Let H be a subgroup of G. Put*

$$\Omega = \{\, aH \mid a \in G \,\}.$$

Then Ω is a partition of G.

Lemma 12. *Let H be a subgroup of G and let $a \in G$. Then the function $f_a : H \to aH$ defined by $f_a(h) = ah$ is a bijection.*

Theorem 13. *Let G be a finite group and let H be a subgroup of G. Then $|G|$ is a multiple of $|H|$.*

Thursday: The Real Numbers

In this final section of the course we will study the real numbers. You are already familiar with a number of theorems about the real numbers: rules for n^{th} root test for determining whether a series converges, the mean value theorem, and so on. We will be learning how to prove theorems like these.

Of course, the first thing we have to do is to establish our assumptions, or *axioms*, and agree that (at least in principle) everything we prove about the real numbers should come **only** from these axioms and not from any pictures we have of how the real numbers look and behave. We will give axioms which say that the real numbers are a *complete, ordered field.* There are lots of examples of fields, some of which are ordered fields. However, we will see that there is, up to isomorphism, only one complete ordered field. By "up to isomorphism", we mean that if R and S are both complete ordered fields, then there is an isomorphism from R to S. In fact, in this case we can do even better: not only is there at least one isomorphism from R to S, but that isomorphism is unique.

The field axioms [8.2]

Definition. *A* field *is a set F equipped with two binary operations, addition $+$ and multiplication $\cdot$ (as usual, we often omit the $\cdot$ and write $x \cdot y$ as xy) and distinct elements 0_F and 1_F with the properties that*

- *$+$ and $\cdot$ are associative and commutative operations on F;*
- *0_F is an identity for $+$ and 1_F is an identity for $\cdot$;*
- *$\cdot$ distributes over $+$, i.e. for all $x, y, z \in F$ we have $x(y + z) = xy + xz$;*
- *every $x \in F$ has an additive inverse $-x$; and*
- *every $x \in F \setminus \{0_F\}$ has a multiplicative inverse $\frac{1}{x}$.*

Example 14. *The real numbers $\mathbb{R}$, with the usual addition, multiplication, 0 and 1, form a field.*

Example 15. *Let $F = \{E, 0\}$, with $+$ and $\cdot$ defined by the Cayley Tables*

$+$	E	O
E	E	O
O	O	E

and

$\cdot$	E	O
E	E	E
O	E	O

(Note: it may help to think of E and O as "even" and "odd" respectively). Then F is a field, with 0_F being the element E and 1_F being the element O.

Exercise 16. *In the previous example, what are $-E$, $-O$ and $\frac{1}{O}$?*

Example 17. *Let p be a prime number. Then $\mathbb{Z}_p$ is a field, with $+$ and $\cdot$ being $+_p$ and $\cdot_p$ respectively, and 0_F and 1_F beling $\overline{0}$ and $\overline{1}$ respectively.*

Exercise 18. *Write up the Cayley Tables for $+_7$ and $\cdot_7$. For each n with $0 \leq n \leq 6$ identify $-\overline{n}$ and for each n with $1 \leq n \leq 6$ identify $\frac{1}{\overline{n}}$.*

Just as when we wrote down axioms for $\mathbb{Z}$ and $\mathbb{N}$, we can deduce many familiar facts about a field from these axioms.

Proposition 19. *Let F be a field. For every $x \in F$ we have $0_F x = 0_F$ and $-(-x) = x$.*

However, the field axioms do **not** allow us to prove the familiar fact that for all $x \neq 0_F$ we have $x \neq -x$.

Finally, a little notation: if F is a field and $x, y \in F$, we write $x - y$ for $x + (-y)$, and $x \div y$ or $\frac{x}{y}$ for $x \cdot \frac{1}{y}$.

Friday: The Order Axioms for $\mathbb{R}$

Axioms for an ordered field [8.3]

Definition. *An* ordered field *is a field F with a subset P such that*

- *if $x, y \in P$ then $x + y \in P$ and $xy \in P$;*
- *for all $x \in F$, exactly one of the following holds:*
  - ○ *$x \in P$; or*
  - ○ *$x = 0_F$; or*
  - ○ *$-x \in P$.*

We will see shortly why we use the term "ordered" (and why we use the letter P). First, we will see some consequences of these axioms.

Proposition 20. *Let F be an ordered field. Then for all $x \in F \setminus \{0_F\}$, $x \neq -x$.*

Proposition 21. *Let F be an ordered field. Then for all $x \in F \setminus \{0_F\}$, $x^2 \in P$. In particular, $1_F \in P$.*

Proposition 22. *The field $\mathbb{Z}_p$ (for p a prime number) is not an ordered field, in other words there is no subset P of $\mathbb{Z}_p$ which satisfies the ordered field axioms.*

Example 23. *The real numbers are an ordered field, with $P = \{ x \in \mathbb{R} : x > 0 \}$.*

Proposition 24. *Let F be an ordered field. Define relations $<$ and $\leq$ on F by declaring that, for $x, y \in F$, $x < y$ iff $y - x \in P$, and $x \leq y$ iff $x < y \vee x = y$. Then $\leq$ is a total order on F.*

Whenever we have an ordered field F, we will always assume $<$ and $\leq$ are the relations defined in the above proposition.

Proposition 25. *Let F be an ordered field. Let $a, b, c, d \in F$.*

1. *If $a < b$ then $a + c < b + c$.*
2. *If $a \leq b$ then $a + c \leq b + c$.*
3. *If $a < b$ and $0_F < c$ then $ac < bc$.*
4. *If $0_F < a < b$ then $0_F < \frac{1}{b} < \frac{1}{a}$.*

Example 26. *The rational numbers $\mathbb{Q}$ are an ordered field, with the usual $+$, $\cdot$, 0 and 1, and with $P = \{ q \in \mathbb{Q} : q > 0 \}$.*