

Last lecture

- The ring of **Gaussian integers** is the subring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ of \mathbb{C} . $\mathbb{Z}[i]$ is a principal ideal domain.
- If $a, b \in R$ then a **divides** b , or b is a **multiple** of a , if $b = at$ for some $t \in R$. We write $a|b$.
- A **unit** is any element of R which has an inverse.
- a and b are **associates** if $a = bu$ for some unit $u \in R$. Being associates defines an equivalence relation on R .
- If R an integral domain then $b|a \iff aR \subseteq bR$.
- If R an integral domain then a and b are associates $\iff a|b$ and $b|a \iff aR = bR$.
- A **greatest common divisor** of a and b is any $d \in R$ such that $d|a$, $d|b$ and $e|d$ whenever $e|a$ and $e|b$. Any two GCDs are associates.
- If R is a PID then $d = \gcd(a, b) \iff aR + bR = dR$.

This lecture

Zorn's Lemma — a mathematical interlude.

Zorn's lemma

Question

Suppose that G is an **infinite group** and $1 \neq g \in G$.
Is there a subgroup H which is maximal such that $g \notin H$?
That is, can we find a subgroup H such that $g \notin H$ and whenever $H \subsetneq K$ then $g \in K$?

For **finite groups** this trivially true.

To answer questions like this for infinite groups, rings, fields, ... we need the **Axiom of choice**, or **Zorn's lemma**.

Definition 13.1 (Some definitions)

- A relation \sim **anti-symmetric** if $a \sim b$ and $b \sim a \implies a = b$.
- A **preorder** on S is a relation which is reflexive and transitive.
- A **partial order** \leq on S is an anti-symmetric preorder.
- A **total order** on S is a partial order such that either $a \leq b$ or $b \leq a$, for all $a, b \in S$.

Examples of preorders and total orders

- $S = \mathbb{N} = \{0, 1, 2, 3, \dots\}$ with $a \leq b \iff a|b$.
Then \leq is a partial order.
- $S = \mathbb{Z}$ with $a \leq b \iff a|b$.
Then \leq is a preorder.
- $\mathcal{P} = \{Y | Y \subseteq X\}$, the set of subsets of X , with $Y \leq Z$ if $Y \subseteq Z$.
Then \mathcal{P} is a partially ordered set.
- $S = \mathbb{R}$ with $r \leq s$ if r is less than or equal to s .
Then \mathbb{R} is totally ordered by \leq .

Remark

Any preorder \leq gives rise to an equivalence relation \sim where $x \sim y$ if $x \leq y$ and $y \leq x$. (**Check!**)

This is a very useful and important construction, however, in this course we won't ever need it.

Zorn's lemma

An **upper bound** for $A \subseteq S$ is an element $s \in S$ such that $a \leq s, \forall a \in A$.
A **maximal element** in S is an element $m \in S$ such that $s \leq m, \forall s \in S$.
A subset of S is **totally ordered** if \leq restricts to a total order on it.

Zorn's lemma

Suppose that (S, \leq) is a partially ordered set such that **every** totally ordered subset of S has an upper bound.
Then S has a maximal element.

Remarks

- Zorn's lemma says that S has **at least one** maximal element.
- The upper bound on a totally ordered subset A belongs to S and not necessarily to A .
- There are literally hundreds of equivalent statements to Zorn's lemma, including the **Axiom of Choice**. In practice, Zorn's lemma is the most convenient form of the Axiom of Choice to apply.
- Even though it is called a **Lemma**, this is an **additional assumption** that we impose on top of the usual axioms of set theory/mathematics.

An application of Zorn's lemma to maximal subgroups

Theorem 13.2

Suppose that G is a group and $1 \neq g \in G$. Then there exists a maximal subgroup H of G which does **not** contain g .

Proof Let \mathcal{S} be the set of subgroups of G which do **not** contain g . Then \mathcal{S} is partially ordered by inclusion: $S \leq T$ if $S \subseteq T$. Since $g \neq 1$, the trivial subgroup $\{1\} \in \mathcal{S} \implies \mathcal{S} \neq \emptyset$. It is enough to show that \mathcal{S} has a maximal element.

Let \mathcal{H} be any totally ordered subset of \mathcal{S}

That is, \mathcal{H} is a (possibly infinite) collection of subgroups

$$\dots \subseteq H_{-1} \subseteq H_0 \subseteq H_1 \subseteq \dots$$

Set $K = \bigcup_{H \in \mathcal{H}} H$.

Then K is a subgroup of G as the union of a collection of subgroups is again a subgroup, $g \notin K$ and $H \subseteq K$ for all $H \in \mathcal{H}$.

Hence, $K \in \mathcal{S}$ and K is an upper bound for \mathcal{H} .

Therefore, **by Zorn's lemma**, \mathcal{S} has a maximal element, as required. \square

Challenge exercise

Exercise Use Zorn's lemma to prove that any partial order on a set can be extended to a total order.

That is, if (S, \leq) is a partially ordered set then there exists a total order \preceq on S such that $x \leq y \implies x \preceq y$.

This is quite tricky: you need to put a partial order on the set of 'partial extensions' \preceq' of \leq to a total order.

This exercise gives one half of showing that Zorn's lemma is equivalent to the well ordering principal

The Well Ordering Principal

Every partial order on a set can be extended to a total order.

We do actually need the Axiom choice in this course, but we do need some ideas which are very closely related to it.

Zorn's lemma and the Well Ordering principal are both equivalent to the Axiom of Choice. The next slide gives more equivalent statements.

Equivalent forms of the Axiom of choice

The Axiom of Choice

Let \mathcal{S} be a collection of non-empty sets. Then we can choose an element from each set in \mathcal{S} . That is, there exists a function f on \mathcal{S} such that $f(S) \in S$, for all $S \in \mathcal{S}$.

The following statements are equivalent to the axiom of choice:

- Every vector space has a basis.
- Every non-trivial ring with one has a maximal ideal.
- Every field has an algebraic closure.
- If A is infinite then A and $A \times A$ have the same cardinality.
- Every surjective function has a right inverse.
- In any partially ordered set, every totally ordered subset is contained in a maximal totally ordered subset.
 - In the product topology, the closure of a product of subsets is equal to the product of the closures.
 - If A and B are sets then either they have the same cardinality or one has smaller cardinality than the other.

The ascending chain condition on ideals

Definition 13.3

A ring R satisfies the **ascending chain condition** on ideals if every **increasing** chain of ideals stabilizes.

That is, whenever $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ is a chain of ideals then

$$I_n = I_{n+1} = I_{n+2} = \dots \text{ for some } n.$$

Similarly, R satisfies the **descending chain condition** on ideals if every **decreasing** chain of ideals stabilizes.

Example The ring \mathbb{Z} of integers satisfies the ascending chain condition on ideals but fails the descending chain condition.

If $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ is a chain of ideals in $\mathbb{Z} \implies I_i = n_i \mathbb{Z}$, for $n_i \geq 0$

$$\implies \dots |n_{i+1}| |n_i| \dots |n_2| |n_1|$$

$$\implies \text{there exists an integer } n | n_1 \text{ such that } n_i = n, \text{ for } i \gg 0$$

$$\implies I_i = n\mathbb{Z}, \text{ for } i \gg 0.$$

Conversely, the chain $\mathbb{Z} \supset p\mathbb{Z} \supset p^2\mathbb{Z} \supset p^3\mathbb{Z} \supset \dots$ does not stabilize.