MATH H113: Honors Introduction to Abstract Algebra

2016-03-30

- Maximal & prime ideals
- Zorn's lemma

Homework due 2016-04-15:
Sect. 7.4: 14, 27, 36
Sect. 7.5: 2, 3, 4

Homework due 2016-04-18:
Extra assignment (see sheet).

Example: Ideals in $\mathbb{Z}$.
Let I be an ideal in $\mathbb{Z}$. Then it's an additive subgroup:
$I = m\mathbb{Z} = \langle m \rangle = \{mn : n \in \mathbb{Z}\} = (m)$ (this is an ideal (principal ideal)).
So $\{\text{ideals of ideals of } \mathbb{Z}\} = \{(m) : m \in \mathbb{N}\}$. Also: every ideal of $\mathbb{Z}$ is principal.
What about the ideal (a, b) in $\mathbb{Z}$?

Note: $(d) \leq (a) \iff d \in (a) \iff a \mid d$
So, $(a, b) \leq (d) \iff a \in (d)$ and $b \in (d)$
$\iff d \mid a$ and $d \mid b$
$\iff d$ is a common divisor of a and b.
Now $(a, b) = (m)$ where m is the largest number that $(a, b) \leq m$ so m is the largest common divisor of a and b, $m = \gcd(a, b)$.
So (a, b) (ideal generated by a and b) $= ((a, b))$ (principal ideal generated by $\gcd(a, b) = (a, b)$).
Recall: An ideal of M in a ring R is said to be maximal if:

i. $M \neq R$, and
ii. there are no ideals M' *strictly between* M and R: $M \subsetneq M' \subsetneq R$.

Proposition: Let R be a commutative ring with 1, and let M be an ideal in R. Then M is maximal $\iff$ R/M is a field.
Recall: R/M is a field $\iff$ R/M is commutative (always true (because R is commutative)), R/M has $1 \neq 0$ (R/M always has 1 (since R has 1)) and all nonzero elements of R/M are units (proved last time: If R/M has $1 \neq 0$, then it's a field $\iff$ it's commutative its only ideals are (0) and (1) $\iff$ only ideals are (0) and (1) (assuming the other conditions are true)).
So this is true
$\iff R/M \neq 0$
$\iff M \neq R \iff$ the only ideals of M' with $M \subseteq M' \subseteq R$ are M and R.

Definition: Let R be a commutative ring with 1. An ideal P of R is *prime* if

i. $P \neq R$ and
ii. for all $x, y \in R$, $xy \in P \implies x \in P$ or $y \in P$

Proposition: Let R be as above. Then an ideal P of R is prime $\iff$ R/P is an integral domain.

Proof: R/P is an integral domain if and only if:

i. R/P is commutative,
ii. R/P has $1 \neq 0$, and
iii. R/P has no zero divisors
Again, (i) is automative, and (ii) $\iff$ ¶ $\neq R$

(iii) $\iff$ $\bar{x}\bar{y} = \bar{0} \implies \bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$ $\forall \bar{x}, \bar{y} \in R/P$ ($\bar{x}$ means $x \in R$ and $\bar{x} = x + P$) $\iff$ $xy \in P \implies x \in P$ or $y \in P$ $\forall x, y \in R$.

Corollary: Let R be a commutative ring with 1. Then all maximal ideals of R are prime.
Proof: Let M be an ideal of R. THen M is maximal $\iff$ R/M is a field $\implies$ R/M is entire (= integral domain) $\iff$ M is prime.
Example: Maximal and prime ideals in $\mathbb{Z}$. Let I be an ideal in $\mathbb{Z}$. THen $I = (m)$ for some $m \in \mathbb{N}$.
$m = 0$: Then $\mathbb{Z}/I = \mathbb{Z}/(0) \cong \mathbb{Z}$, which is an integral domain but not a field. So (0) is prime but not maximal ($(0) \subsetneq (2) \subsetneq (1)$).
$m \neq 0$: If m is prime then $(\mathbb{Z}/(m))^\times = \mathbb{Z}/m\mathbb{Z} \setminus \{\bar{0}\}$ so $\mathbb{Z}/m\mathbb{Z}$ is maximal, and prime. (or: $(m) \subsetneq (n) \subsetneq 1 \iff 1 < n < m$ and $n \mid m$ so this shows that if m is composite then (m) is not maximal. If m is not prime then either $m = 1$ ($\implies (m) = \mathbb{Z}$, so (m) is not prime) or $m = ab$ with $a, b > 1$, so $a, b \notin (m)$ but $ab \in (m)$, so (m) is not prime.
$\therefore$ (m) is prime $\iff$ m is prime or $m = 0$
(m) is maximal $\iff$ m is prime

Zorn's Lemma

Definition: Let A be a set. Then a *partitial ordering* on A is a relation $\leq$ on A that is:

1. reflexive ($x \leq x$ $\forall x \in A$),
2. antisymmetric ($x \leq y$ and $y \leq x$, then $x = y$, $\forall x, y \in A$), and
3. transitive (if $x \leq y$ and $y \leq z$ then $x \leq z$, $\forall x, y, z \in A$).

A total ordering on A is a partial ordering $\leq$ on A such that, $x \leq y$ or $y \leq x$ $\forall x, y \in A$. A partially ordered set is a set with a partial ordering on it (this is also called a *poset*). *Totally ordered set* is defined similarly.

Examples: - $\mathbb{R}$ is totally ordered under the usual $\leq$. - The set of subgroups of a group is partially ordered under $\leq$ (but not under $\trianglelefteq$ (not transitive)). - Any collection of sets is partially ordered under $\subseteq$

Definition: Let A be a partially ordered set. Then:

1. a *chain* in A is a totally ordered subset of A (same ordering as on A)
2. an *upper bound* for any subset $B \subseteq A$ is an element $m \in A$ such that $x \leq m$ $\forall x \in B$
3. A *maximal element* of A is an element $m \in A$ such taht $m \leq x \implies x = m$ $\forall x \in A$.

Examples: A maximal ideal in a ring R is a maximal element in the set of all proper ($\neq R$) ideals of R. There may be many of these. If $A = \emptyset$ then there is exactly one relation on A, and it is a total ordering on A. $\therefore \emptyset$ is a poset, and for any poset A, $\emptyset \subseteq A$ is a chain in A.
Incidentally: if A is a poset, then a largest element of A is an element $M \in A$ such that $x \leq M$ $\forall x \in A$. There is at most one of these. largest $\implies$ maximal.

Zorn's Lemma: Let A be a nonempty partially ordered set, in which every nonempty chain has an upper bound. Then A has a maximal element.