Math 510B Notes

Peter Kagey

Monday, January 7, 2019

Lemma. (Zorn's Lemma)
Let $\mathscr{S}$ be a nonempty partially ordered set. If every chain of subsets $S_1 \preceq S_2 \preceq \dots$ in $\mathscr{S}$ has an upper bound in $\mathscr{S}$, then $\mathscr{S}$ contains a maximal element.

Notation. Let R denote a commutative ring with 1.

Corollary. (to Zorn's Lemma)
If $1 \in R$ and $I \neq R$ is any proper ideal of R (left, right, or two-sided), then there exists a maximal ideal M such that $I \subseteq M \subset R$.

Note. This corollary does not hold for rings without 1.

Proof. Let $\mathscr{S}_I = \{J : I \subseteq J \text{ and } J \text{ is a proper ideal of } R\}$ be the set of proper ideals of R that contain I. Then any chain $\{S_n\}$ has an upper bound in $\mathscr{S}_I$, namely $\bigcup_n S_n$, so by Zorn's Lemma, $\mathscr{S}_I$ contains a maximal element.

Notice that for all $S \in \mathscr{S}_I$, $1 \notin S$ (otherwise $S = R$). Thus $\bigcup_n S_n$ is a proper subset of R, so it is enough to show that it is an ideal. Notice that for any $x, y \in \bigcup_n S_n$ there exists some N such that $x, y \in S_N$. Thus

1. $\bigcup_n S_n$ is closed because $x + y \in S_N \subseteq \bigcup_n S_n$, and
2. $\bigcup_n S_n$ is an ideal because for all $r \in R$, $xr \in S_N \subseteq \bigcup_n S_n$.

□

Lemma. Let R be a commutative ring with unity. Then M is a maximal ideal if and only if R/M is a field.

Proof.
($\Longrightarrow$) Assume that M is a maximal ideal, and let choose $r \notin M$ so that $\bar{r} = r + M \neq \bar{0}$. Then the set $M + rR = \{m + r \cdot s : m \in M, s \in R\}$ is an ideal of R (check) and M is a proper subset of $M + rR$, so by the maximality of M, $M + rR = R$, and thus there exists some $m \in M$ and $s \in R$ such that $m + r \cdot s = 1$. Thus in the quotient, $\bar{r} \cdot \bar{s} = \bar{1}$, and so $\bar{r}$ is invertible, and R/M is a field.

($\Longleftarrow$) Assume that R/M is a field. (...) □

Definition. (Prime ideal)
Assume R is a commutative ring. Then a proper ideal $P \lhd R$ is called a prime ideal if $ab \in P$ then either $a \in P$ or $b \in P$.

Lemma. P is a prime ideal of R if and only if R/P has no zero divisors.

Proof.
($\Longrightarrow$) Assume that P is a prime ideal of R. For the sake of contradiction, also assume that $\bar{a}, \bar{b} \in R/P$ with $\bar{a}\bar{b} = \bar{0}$. Thus $(a + P)(b + P) \subseteq P$, and so $ab \in P$ (check).
By hypothesis, since P is a prime ideal, $a \in P$ or $b \in P$, so $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. Thus R/P has no zero divisors.

($\Longleftarrow$) Assume that R/P has no zero divisors. Let $ab \in P$, and consider $(a+P)(b+P) = ab + aP + Pb + P \in R/P$. Since $ab \in P$, $\bar{a} \cdot \bar{b} = \bar{0} \in R/P$. Since R/P has no zero divisors, $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$ and thus $a \in P$ or $b \in P$. Therefore P must be a prime ideal. □

Example. Let $R = \mathbb{Z}$. Then any prime ideal $P = \langle p \rangle = \mathbb{Z}/p\mathbb{Z}$, so all nonzero prime ideals are maximal.

Example. Let $R = k[x]$ for some field k. Then any prime ideal $P = \langle f(x) \rangle = f(x) \cdot k[x]$ for some irreducible polynomial f, so all nonzero prime ideals are maximal.

Example. Let $R = k[x, y]$ for some field k. Then $P = \langle x \rangle = xR$ is a prime ideal since $R/\langle x \rangle \cong k[y]$ is a domain, but it is **not maximal** because $k[y]$ is not a field.

Definition. A (not necessarily commutative) ring R is called a domain if it has the zero-product property. That is if $ab = 0$ implies that $a = 0$ or $b = 0$.

Definitions. Let R be a commutative ring with unity.

1. A ring R is called a principal ideal domain (PID) if for every $I \subset R$ there exists $a \in I$ so that $I = aR = \langle a \rangle$.
2. If $a, b \in R$ then $c = \gcd(a, b)$ is the greatest common divisor of a and b if
   (a) $c|a$ and $c|b$ (i.e. there exists some x such that $a = cx$, etc.), and
   (b) if $d \in R$ divides a and b then $d|c$.
3. A unit $u \in R$ is an invertible element.
4. Two elements $a, b \in R$ are associates if there exists a unit u such that $a = bu$.
5. An element $a \in R$ is irreducible if whenever $a = bc$ for $b, c \in R$ then either b or c is a unit.
6. An element $p \in R$ is a prime element if whenever $p|ab$ then $p|a$ or $p|b$.
7. R is a unique factorization domain (UFD) if every element $a \in R$ may be written as a product of irreducible elements which are unique up to being associates. That is if $a = q_1 q_2 \dots q_r = t_1 t_2 \dots t_r$, then up to reordering, $q_i = u_i t_i$ where u_i is some unit.

Claim. $I = \langle p \rangle$ is a prime ideal if and only if p is a prime element.

Lemma. A prime element is irreducible when R is a domain.

Proof. Assume $p = ab$. Since p is prime, $p|a$ or $p|b$. (Assume $p|a$ WLOG). So $a = px$, thus $p = (px)b$ and $1 = xb$ by the cancellation property. Thus b is a unit and hence p is irreducible. □

Example. The ring of polynomials over a ring in n variables, $k[x_1, \dots, x_n]$ is a unique factorization domain (UFD).

Lemma. Let R be a PID. Then gcds exist and $\langle \gcd(a, b) \rangle = \langle a \rangle + \langle b \rangle$.

Exercise. Prove this lemma when $R = \mathbb{Z}$.