Prime and maximal ideals

Sergei Silvestrov

Spring term 2011, Lecture 7

Contents of the lecture

Prime and maximal ideals.
Maximal ideals

Definition 1. (Sec 6.3, p. 157)
An ideal $M$ in a ring $R$ is said to be maximal if $M \neq R$ and for every ideal $N$ such that $M \subseteq N \subseteq R$, either $N = M$ or $N = R$.

Example 1. The ideal $3\mathbb{Z}$ is maximal in $\mathbb{Z}$, but the ideal $4\mathbb{Z}$ is not since $4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Example 2. (p. 156)
The quotient ring $\mathbb{Z}[x]/(x)$ is not a field. Furthermore, the ideal $I$ of polynomials with even constant terms lies strictly between the ideal $(x)$ and $\mathbb{Z}[x]$, that is,

$$(x) \subsetneq I \subsetneq \mathbb{Z}[x]$$

Maximal ideals may be characterised in terms of their factor rings.

Theorem 1. (Th 6.15, Sec 6.3, p. 156)
Let $M$ be an ideal in a commutative ring $R$ with unity $1 \neq 0$. 
Then $M$ is maximal if and only if the factor ring $R/M$ is a field.

Corollary 1. The following conditions on a commutative ring $R$ with unity $1 \neq 0$ are equivalent.

1. $R$ is a field.
2. $R$ has no proper nontrivial ideals.
3. $0$ is a maximal ideal in $R$.

Proof. $R$ is isomorphic to $R/0$ and is a field if and only if $0$ is maximal. But clearly $0$ is maximal if and only if $R$ has no proper nontrivial ideals. \qed
Prime ideals

**Definition 2.** (Sec 6.3, p 154)
An ideal $P \neq R$ is said to be **prime** if for all $a, b \in R$ $ab \in P$ implies $a \in P$ or $b \in P$.

**Example 3.** The zero ideal in any integral domain is prime since $ab = 0$ if and only if $a = 0$ or $b = 0$.

**Example 4.** If $p$ is a prime integer, then the ideal $p\mathbb{Z}$ is prime since $ab \in p\mathbb{Z}$ means that $p$ divides $ab$, then $p$ divides $a$ or $p$ divides $b$, which means that $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

**Theorem 2.** (Th 6.14, Sec 6.3, p 155)
In a commutative ring $R$ with unity $1 \neq 0$ an ideal $P$ is prime if and only if the factor ring $R/P$ is an integral domain.

*Proof.* $R/P$ is a commutative ring with unity $1 + P$ and zero element $0 + P = P$ by Theorem 2.7.8.

If $P$ is prime, then $1 + P \neq P$ since $P \neq R$. Furthermore, $R/P$ has no zero divisors since

$$(a + P)(b + P) = P \Rightarrow ab + P = P$$

$$\Rightarrow ab \in P$$

$$\Rightarrow a \in P \text{ or } b \in P$$

$$\Rightarrow a + P = P \text{ or } b + P = P.$$ 

Therefore, $R/P$ is an integral domain.

Conversely, if $R/P$ is an integral domain, then $1 + P \neq 0 + P$, whence $1 \notin P$. Therefore, $P \neq R$. Since $R/P$ has no zero divisors,

$$ab \in P \Rightarrow ab + P = P$$

$$\Rightarrow (a + P)(b + P) = P$$

$$\Rightarrow a + P = P \text{ or } b + P = P$$

$$\Rightarrow a \in P \text{ or } b \in P.$$ 

Therefore, $P$ is prime. 

**Corollary 2.** (Th 6.16, Sec 6.3, p 157) If $R$ is a commutative ring with unity $1 \neq 0$, then every maximal ideal $M$ in $R$ is prime.

*Proof.* By Theorem 1, $R/M$ is a field, hence an integral domain. By Theorem 2, $M$ is prime. 

---

– Typeset by Foil\TeX –
Theorem 3. If $F$ is a field, then either it is of prime characteristic $p$ and contains a subfield isomorphic to $\mathbb{Z}_p$ or it is of characteristic 0 and contains a subfield isomorphic to $\mathbb{Q}$.

Proof. Consider the ring homomorphism $\varphi : \mathbb{Z} \to F$ defined by $\varphi(n) = n \cdot 1$. The kernel $\ker(\varphi)$ must be an ideal in $\mathbb{Z}$. All ideals in $\mathbb{Z}$ are of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$.

If $m = 0$, then $\varphi$ is one-to-one, and so there is an isomorphic copy of $\mathbb{Z}$ that is a subring of $F$. Its field of quotients is $\mathbb{Q}$ and is a minimal field containing the above mentioned subring. So $F$ must contain a subfield isomorphic to $\mathbb{Q}$ and has characteristic 0.

If $m \neq 0$, the First Isomorphism Theorem gives $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\varphi[\mathbb{Z}] \subseteq F$. Since $F$ is a field, $\varphi[\mathbb{Z}]$ is a domain, and so $m$ is a prime $p$. Now

$$\varphi[\mathbb{Z}] = \{0, 1, 2 \cdot 1, \ldots, (p - 1) \cdot 1\}$$

is a subfield of $F$ isomorphic to $\mathbb{Z}_p$, and the characteristic of $F$ is $p$.  

Definition 3. The fields $\mathbb{Q}$ and $\mathbb{Z}_p$ are prime fields.
Principal ideals

**Definition 4.** Let $R$ be a commutative ring with unity $1 \neq 0$. The ideal $\{ ra : r \in R \}$ is called the **principal ideal generated by** $a \in R$ and is denoted by $\langle a \rangle$. An ideal $N$ is called **principal** if there exist $a \in R$ such that $N = \langle a \rangle$.

**Theorem 4.** If $F$ is a field, then every ideal in $F[x]$ is principal.

**Theorem 5.** The maximal ideals in $F[x]$ are the ideals $\langle f(x) \rangle$ generated by irreducible polynomials $f(x)$. 
Our basic goal and outline of its achieving

We would like to prove the following: let $F$ be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. There exist a field $E$ containing both $F$ and a zero $\alpha$ of $f(x)$.

**Sketch of proof.**

1. Choose an irreducible factor $p(x)$ of $f(x)$ in $F[x]$ (nothing to do if $p(x)$ does not exist).
2. By Theorem 5, the ideal $\langle p(x) \rangle$ is maximal. By Theorem 1, the factor ring $E = F[x]/\langle p(x) \rangle$ is a field.
3. Find an isomorphism between $F$ and a subfield in $E$.
4. Put $\alpha = x + \langle p(x) \rangle \in E$. Prove that $\Phi_\alpha(f(x)) = 0$. That is, $\alpha$ is a zero of $f(x)$ in $E$. 

$\square$