Part V (§26-28)
Ideals and Factor Rings

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

26 Homomorphisms and Factor Rings

As always, a homomorphism $f : X \longrightarrow Y$ between two sets X, Y with **a given structure**, is a map f that **respects** the structure. Accordingly, homomorphisms of rings was define in §18, which we reall.

Definition 26.1. *A map $\varphi : R \longrightarrow R'$ from a ring R to another ring R' is called a* **homomorphism** *of rings, if*

$$\forall\, a, b \in R \quad \varphi(a+b) = \varphi(a)+\varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \textit{and also} \quad \varphi(1) = 1.$$

Example 26.2 (26.2 Projection Homomorphism)**.** Let $R_1, \ldots, R_n$ be rings. Then the $i^{th}-$projection $\pi : R_1 \times R_2 \times \cdots \times R_n \longrightarrow R_i$ sending $(r_1, r_2, \ldots, r_n) \mapsto r_i$ is a homomorphism.

26.1 Properties of Homomorphism

In §13, we discussed the properties of group homomorphisms. In this section we do the same for ring homomorphisms. Given most of the results in §13 on group homomorphisms, there is a version for the ring homomorphisms.

Generic Notations. Unless there is risk of confussion, for any ring R, its additive identity will be denoted by zero 0 and multiplicatiove identity will be denoted by 1.

Theorem 26.3 (Analogue of 13.12)**.** Let $\varphi : R \longrightarrow R'$ be a ring homomorphism. Then,

1. $\varphi(0) = 0$.
2. $\varphi(R)$ is a subring of R'.
3. If S' is a subring of R', then $\varphi^{-1}(S)$ is a subring of R.

Proof. Routine, like the proof of theorem 13.12. Read it from the textbook. ■

Caution: Contrary to the convention in the textbook, all rings in this class that unlity 1.

Definition 26.4. Let $\varphi : R \longrightarrow R'$ be a ring homomorphism. *As in group theory*, we define **kernel of** φ as

$$\ker(\varphi) = \varphi^{-1}(\{0\}).$$

The kernel $\ker(\varphi)$ has the follwoing properties:

1. $\ker(\varphi)$ is a subgroup of the additive group R.
2. Suppose $x \in \ker(\varphi)$ and $a \in R$. Then $ax \in \ker(\varphi)$ and $xa \in \ker(\varphi)$.

Proof. Note, a ring homomorphism is, in particular, a homomorphism of the additive group. So, (1) follows from the corresponding theorem on group homomorphisms (*show it is closed under addition, and the negative*). We also have

$$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0, \quad similalry, \quad \varphi(xa) = 0.$$

So, $ax, xa \in \ker(\varphi)$. The proof is complete. ■

Remark, ignoreable: *I consider such definitions of kernel, to be "ad hoc", while this is the approprite defintion at this level, or for this course. In the language of category theory all "kernels", "cokernel", "images" are defined in a unified manner.*

Theorem 26.5 (Analogue of 13.15)**.** Let $\varphi : R \longrightarrow R'$ be a ring homomorphism and let $H = \ker(\varphi)$. Then, $\varphi^{-1}(\varphi(a)) = a + H$, where $a + H$ is the coset of the additive subgroup H, that contains a.

Proof. Apply theorem 13.15 or repeat its proof. ∎

Corollary 26.6 (Analogue of 13.18)**.** $\varphi : R \longrightarrow R'$ be a ring homomorphism. Then φ is injective if and only if $\ker(\varphi) = \{0\}$.

Proof. Apply theorem 13.18 or repeat its proof. ∎

26.2 Factor (Quotient Rings)

Before we proceed, I want to define "ideals" of a ring, by abstracting the properties of kernels stated in (26.4). (*The textbook postpones it a little longer*).

Definition 26.7 (26.10)**.** *Let R be a ring. An additive subgroup N of R is called an* **ideal** *of R, if*

$$\forall a \in R \qquad aN \subseteq N, \qquad \textit{and} \qquad Na \subseteq N.$$

Obvious Examples and Comments:

1. By the properties of the kernels (26.4), $\ker(\varphi)$ is an ideal of R, for any ring homomorphism $\varphi : R \longrightarrow R'$.
2. **Trivial Examples:** $\{0\}$ and R are two trivial ideals of a ring R.
3. Suppose N is an ideal of a ring R. If $1 \in N$, then $N = R$.

Definition 26.8. Suppose N is an ideal of a ring R.

1. An ideal N of a ring R is an additive subgroup of R. So, (left) cosets are defined.
2. Since addition is commutative, N is a normal subgroup of R. So, left and right cosets are same.
3. For $a \in R$, the coset is denoted by

$$a + N \qquad \textit{or} \qquad \overline{a} \quad \text{(when N is understood from context)}$$

4. Set of all such cosets are denoted bt R/N. By group theory, R/N is a commutative groups under the addition, defined, for $a, b \in R$, by

$$(a + N) + (b + N) = (a + b) + N$$

Lemma 26.9 (26.14)**.** *Suppose N is an ideal of a ring R. Define multiplication, for $a, b \in R$, by*

$$(a+N)(b+N) = (ab)+N.$$

Then, multiplication is well defined and R/N form a ring under the usual addition and this multiplication.

Proof. Suppose $a+N = x+N$ and $b+N = y+N$. We will prove $ab+N = xy+N$. Now, $a = x+h_1, b = y+h_2$ for some $h_1, h_2 \in H$. So, $ab = xy + (xh_2 + h_1y + h_1h_2) \in xy+N$. So, $ab+N = xy+N$. So, this multiplication is well defined.

From group theory, R/N is an additive group. Regarding the multiplication

1. For $a, b, c \in R$ we have
$$((a+N)(b+N))(c+N) = (ab+N)(c+N) = (ab)c+N$$
$$= a(bc)+N = (a+N)((b+N)(c+N)).$$
So, the multiplication is associative.

2. Distributivity: Also,
$$((a+N)+(b+N))(c+N) = (ac+bc)+N = (ac+N)+(bc+N)$$
$$= (a+N)(c+N)+(b+N)(c+N)$$
Likewise,
$$(c+N)((a+N)+(b+N)) = (c+N)(a+N)+(c+N)(b+N).$$
So, distributiviy holds.

3. Also, if $N \neq R$, then $1+N$ is the unity in R/N, because
$$(a+N)(1+N) = a+N = (1+N)(a+N).$$
If $N = R$, then $R/N = \{0\}$ is the one element group.

The proof is complete. ∎

Definition 26.10. Let R and N be above. Then the ring R/N is called the **factor ring** (or **quotient ring**). R/N is also denoted by $\frac{R}{N}$.

26.3 Fundamental Homomorphism Theorem

Theorem 26.11 (Analogue of 14.9)**.** *Let N be an ideal of a ring R. Then, $\gamma : R \longrightarrow R/N$ is a homomorphism of rings.*

Proof. As in group theory, for $a \in$ define $\gamma(a) = a + N \in R/N$.

From group theory (14.9) or directly, γ is well defined and

$$\gamma(a+b) = (a+b) + N = (a+N) + (b+N) = \gamma(a) + \gamma(b)$$

Also,

$$\gamma(ab) = (ab) + N = (a+N)(b+N) = \gamma(a)\gamma(b).$$

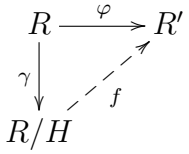
Further,

$$\gamma(1) = 1 + N$$

is the "one" of R/N. The proof is complete. ∎

Theorem 26.12 (26.17 Analogue of 14.11)**.** Let $\varphi : R \longrightarrow R'$ be a homomorphism of rings and $H = \ker(\varphi)$. Let $\gamma : R \longrightarrow R/H$ be the "canonical" homomorphism defined above. Then,

1. There is a homomorhism $f : R/H \longrightarrow R'$ of rings, such that $\varphi = f\gamma$. Diagramtically,

   commutes.

   We say, φ **factors through** R/H**.**

2. In fact, f is injective.

3. f induces and isomorphism $R/H \xrightarrow{\sim} \varphi(R)$ from R/H to image of φ.

Proof. Only statement that is not group theoretic, hence does not follow from 14.9, is that f is a ring homomorphism. (*However, if asked in an exam, you will have to give a complete proof.*) So, let me give a proof, which will be line for line repeatation of the proof of (14.9).

First, define $f : R/H \longrightarrow R'$ by $f(a+H) = \varphi(a)$.

1. To see f is well defined, let $x+H = a+H$. So, $x \in a+H$ and $x = a+h$ for some $h \in H$. So,

$$\varphi(x) = \varphi(a+h) = \varphi(a) + \varphi(h) = \varphi(a) + 0 = \varphi(a).$$

So, f is well defines. Also

$$f((a+H)+(b+H)) = f((a+b)+H) = \varphi(a+b) = \varphi(a)+\varphi(b)f(a)+f(b)$$

and

$$f((a+H)(b+H)) = f(ab+H) = \varphi(ab) = \varphi(a)\varphi(b)f(a)f(b)$$

and

$$f(1+H) = \varphi(1) = 1.$$

So, f is a well defined ring homomorphism.

2. Let $f(a+H) = 0$, So, $\varphi(a) = 0$ and $a \in \ker(\varphi) = H$, which is the additive identity of R/H. So, by (26.6) f is injective.

3. Clealy, image of f is $\varphi(R)$. So, f is bijective from R/H to $\varphi(G)$, hence an isomorphism.

The proof is complete. ∎

Following summarizes some of the above.

Theorem 26.13 (Summary)**.** Let R be a ring and $N \subseteq R$ be a subset of R. Then, N is a proper ideal of R if and only if N is the kernel of a ring homomorphism $\varphi : R \longrightarrow R'$.

Proof. If $\varphi : R \longrightarrow R'$ is a ring homomorphism and $N = \ker(\varphi)$, then by (26.4), N is an ideal, Since $\varphi(1) = 1 \;\; 1 \notin N$. So, N is a proper ideal of R.

Conversely, suppose N is a proper ideal of R. Then, N is the kernel of the homomorphism $\varphi : R \longrightarrow R/N$. The proof is complete. ∎

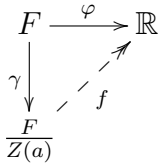
26.4 Some Examples

Example 26.14 (26.19)**.** *Let $n \in \mathbb{Z}$ be an integer $n \geq 2$. Then,*

1. *$n\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$.*
2. *$n\mathbb{Z}$ is the kernel of the homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}_n$.*

Example 26.15. Let F be a ring of all continuous real valued functions on $\mathbb{R}$ and $a \in \mathbb{R}$. Let $Z(a)$ (*"Z " for "zero "*) be the set of all continuous functions in F that vanish at $x = a$.

1. Then, $Z(a)$ is an ideal of F.
2. In fact, $Z(a)$ is the kernal of the evaluation homomorphism $ev_a : F \longrightarrow \mathbb{R}$ that sends $f \mapsto f(a)$
3. By the theorem above or by direct checking ev_a induces an isomorphism $f : F/Z(a) \xrightarrow{\sim} \mathbb{R}$, such that the diagram:



commutes.

More generally, let $U \subseteq \mathbb{R}$ be a subset. Let $Z(U)$ denote all the continuous functions $f \in F$ that vanishes on U. Then, $Z(U)$ is an ideal of F.

Example 26.16. Let R be a commutative ring and $a \in R$. Then Ra is an ideal.

Example 26.17. Let R be a ring and $I \subseteq R$ is an ideal. Then the set $M_n(I)$ of all $n \times n$ matrices with entries in I is an ideal of $M_n(R)$.

Exercise 26.18. *Let F be a field. Prove that $M_n(\mathbb{R})$ has no nontrivial ideal.* (Note this is a noncommutative situation.)

27 Prime and Maximal Ideals

Here are some examples showing how properties of a ring and its factor rings may differ.

Example 27.1 (27.1, 27.10)**.** Let p is a prime number. Then, $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ is field, but $\mathbb{Z}$ is not a field.

In fact, for a positive integer $n \geq 2$, $\mathbb{Z}_n$ is a field if an only if n is a prime.

Example 27.2 (27.2)**.** $\mathbb{Z}\times\mathbb{Z}$ is not an integral domain, because $(1,0)(0,1) = (0,0)$. Let $N = \{(n,0) : n \in \mathbb{Z}\}$. Then, the map $\varphi : \frac{\mathbb{Z}\times\mathbb{Z}}{N} \longrightarrow \mathbb{Z}$ sending $(n,k) + N \mapsto k$ is an isomorphism. So, $\mathbb{Z}/N$ is an integral domain.

27.1 Maximal ideals

Definition 27.3. *Let R be a ring and M be an proper ideal of R. Then M is said to be a* **maximal ideal** *of R, if there is no other ideal N between M and R. That means if,*

$$for\ ideal\ N, \qquad M \subseteq N \Longrightarrow \quad (N = M \quad or \quad N = R).$$

Example 27.4 (28.8)**.** Let p be a (positive) prime integer. Then, $p\mathbb{Z}$ is maximal ideal of $\mathbb{Z}$.

Proof. Suppose N is an ideal of $\mathbb{Z}$ and $p\mathbb{Z} \subseteq N$. Since N is a subgroup of $\mathbb{Z}$, there is a positive integer n such that $N = n\mathbb{Z}$. Since $p\mathbb{Z} \subseteq N = n\mathbb{Z}$, we have $p = nk$. So, $n =$ or $k = 1$. So, $N = n\mathbb{Z} = \mathbb{Z}$ or $N = p\mathbb{Z}$. ∎

Theorem 27.5 (Analogue 15.18)**.** *Let R be a commutative ring* (with unity, as always) *and M be an ideal. Then*

$$M \quad \text{is maximal} \quad \Longleftrightarrow \quad \frac{R}{M} \quad \text{is a field.}$$

Proof. ($\Rightarrow$): Suppose M is maximal ideal. Then, R/M is a commutative ring. Remains to show that each nonzero element in R/M has an inverse. Suppose $a + M \in R/M$ be nonzero. So, $a \notin M$. Now, write $N = Ra + M$ (i.e. *the set* $\{xa + m : x \in R, m \in M\}$). Routine checking shows N is an ideal of R. Now, $M \subseteq N$, and $M \neq N$ because $a \in N$ and $a \notin M$. Since M is maximal, $N = R$. Therfore, $1 \in N = Ra + M$. Write $1 = ba + m$ for some $b \in R$ and $m \in M$. So, $1 + M = (b + M)(a + M)$. Therefore, $b + M$ is the inverse of $a + M$. This completes the proof that R/M is a field.

($\Leftarrow$): Now suppose R/M is field. Suppose N be an ideal and $M \subseteq N$ and $N \neq M$. Required to prove that $M = R$. Since $N \neq M$, there is $a \in N$ such that $a \notin M$. Therefore, $a+M \neq M = \overline{0}$ in R/M. Since R/M is a field, $a+M$ has an inverse $b + M \in R/M$. So, $1 + M = (a + M)(b + M) = ab + M$. So, $1 = ab + m$ for some $m \in M$. Since both $b, m \in N$ we have $1 = ab + m \in N$. Therfore $N = R$. So, M is maximal. The proof is complete. ∎

Corollary 27.6. *A commutative ring R is a field if and only if it has no nontrivial ideals.*

Proof. (*A direct proof is easier. however, let me apply the theorem.*) Suppose R is a field. Since, $R \approx R/\{0\}$, the ideal $\{0\}$ is maximal, by the theorem above. So, other than $\{0\}$, only ideal in R. So, R has only trivial ideals.

Now suppose R has not nontrivial ideals. This means, $\{0\}$ is a maximal ideal. So, $R \approx R/\{0\}$ is a field. The proof is complete. ∎

27.2 Prime ideals

Maximal ideals M of commutative ring R are characterized by the property that R/M is a field. Likewise, prime ideal N will be characterized by the property that R/N is an integral domain. They, also also **like prime numbers**. Recall,

$$\text{for } p \in \mathbb{Z}, p \geq 2 \quad p \text{ is prime} \iff p|mn \implies (p|m \text{ or } p|n).$$

Analogously, define:

Definition 27.7. *Let R be a commutative ring and $N \neq R$ be an ideal R. Then, N is called a* **prime ideal**

$$if \ for \quad a, b \in R, \quad (ab \in N \implies (either \quad a \in N \quad or \quad b \in N))$$

Example 27.8 (27.12)**.** Often the model of a commutative ring is $\mathbb{Z}$. However, in $\mathbb{Z}$, an ideal

$$n\mathbb{Z} \text{ is a prime ideal} \iff n\mathbb{Z} \text{ is a maximal ideal.}$$

Proof. Exercise.

Example 27.9 (27.14)**.** In $\mathbb{Z} \times \mathbb{Z}$ the ideal $\mathbb{Z} \times \{0\}$ and $\{0\} \times \mathbb{Z}$ are prime ideals. More generally, let R be an integral domain. In $R \times R$ the ideal $R \times \{0\}$ and $\{0\} \times R$ are prime ideals.

Proof. We give a proof of the later statement and prove $\mathbb{R} \times \{0\}$ is a prime ideal. First, it is easy to see $\mathbb{R} \times \{0\}$ an ideal and $\mathbb{R} \times \{0\} \neq \times\mathbb{R}$.

Now suppose $(a, b)(x, y) \in \mathbb{R} \times \{0\}$. So, $by = 0$. Since R is an integral domain, $b = 0$ of $y = 0$. So, $(a, b) \in \mathbb{R} \times \{0\}$ or $(x, y) \in \mathbb{R} \times \{0\}$. The proof is complete. ∎

Lemma 27.10. *Let R be a commutative ring. Then,*

$$R \text{ is an integral domain} \iff \{0\} \text{ is a prime ideal.}$$

Proof. Exercise.

Actually, we do not have any interesting example untill we conisder polynomial rings in at least two variables.

Example 27.11. *Suppose F is an field. Let $R = F[x_1, \ldots, x_n]$ be the polynomial ring in n indeterminate. Then,*

1. *$\{0\}$ is a prime ideal.*
2. *$N_r = x_1R + \cdots + x_rR$ is a prime ideal.*
3. *$N_n = x_1R + \cdots + x_nR$ is a maximal ideal.*

Theorem 27.12. *Let R be a commutative ring and $N \neq R$ is an ideal of R. Then,*

$$N \text{ is a prime ideal} \iff \frac{R}{N} \text{ is an integral domain}$$

Proof. ($\Rightarrow$): Suppose N is a prime ideal. Let $(a+N)(b+N) = \overline{0}$. Then, $ab + N = N$. So, $ab \in N$. This implies $a \in N$ or $b \in N$. So, $a + N = \overline{0}$ or $b + N = \overline{0}$. So, R/N is an integral domain.

($\Leftarrow$): Assume R/N is an integral domain. Suppose $ab \in N$. Then, $(a + N)(b + N) = ab + N = \overline{0} = N$. So, $(a + N) = \overline{0}$ or $(b + N) = \overline{0}$. Therefore $a \in N$ or $b \in N$. The proof is complete. ∎

Corollary 27.13. *Let R be a commutative ring. Then, any maximal ideal is a prime ideal.*

Proof. Let M be a maximal ideal. Then, R/M is a field. So, R/M is an integra domain. So, M is a prime ideal ∎

27.3 Prime Fields

Theorem 27.14. *Suppose R is a ring. Then there is a homomorphism*

$$\varphi : \mathbb{Z} \longrightarrow R \quad defined\ by \quad \varphi(n) = n \cdot 1$$

Since, we assume any homomorphism sends $1 \mapsto 1$ this is the only homomorphism $\mathbb{Z} \longrightarrow R$.

Proof. We saw this in §18. ∎

Recall the following definition from §19.

Definition 27.15. *Let R ba a ring with unity 1 (as always). If $n \cdot 1 \neq 0$ for all integsers $n \geq 2$, we say R has* **characteristic** *0.*

If $n \cdot 1 = 0$ for some integser $n \geq 2$ then the the **characteristic** *is defined to be*

$$char(R) = \min\{n \geq 2 : n \cdot 1 = 0\}.$$

So, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ have characteristic zero. $\mathbb{Z}_n$ has characteristic n.

Corollary 27.16. *Suppose R is a ring with $char(R) = n$. Then, R contains a subring isomorphic to $\mathbb{Z}_n$. In particular, if $char(R) = n = 0$ then R contains a subring isomorphic to $\mathbb{Z}$.*

Proof. Consider the homomorphism

$$\varphi : \mathbb{Z} \longrightarrow R \quad defined\ by \quad \varphi(n) = n \cdot 1$$

Then kernel $\ker(\varphi)$ is a sugroup (in fact ideal). So, $\ker(\varphi) = m\mathbb{Z}$, where (from the proof) m is the smallest positive integer in $\ker(\varphi)$. Which means m is the smallest positive integer such that $m \cdot 1 = 0$. By definition of characterisitic $m = n = char(R)$.

By the fundamental theorem, there is an injective homomorphism

$$f : \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow R.$$

So the image of f is a subring of R that is isomorphic to $\mathbb{Z}_n$.

When $char(R) = n = 0$ then $\ker(\varphi) = \{0\}$. So, image of f is isomorphic to $\mathbb{Z}$. The proof is complete. ∎

Theorem 27.17. *Suppose L is a field. Then, $char(L) = p$ is a prime or zero.*

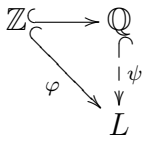
1. *If $char(L) = p$ is prime, then L contains the field $\mathbb{Z}_p$.*
2. *If $char(L) = 0$, then L contains the field $\mathbb{Q}$.*

Proof. Again consider the homomorphism

$$\varphi : \mathbb{Z} \longrightarrow L \quad defined\ by \quad \varphi(n) = n \cdot 1$$

First, assume $char(L) = n > 0$. Let $\ker(\varphi) = n\mathbb{Z}$. We claim n is prime. To see this let $n = rs$, with $r > 0, s > 0$ integers. Then $0 = \varphi(n) = \varphi(r)\varphi(s)$. So, $0 = (r \cdot 1)(r \cdot 1)$. Since, L is integral domain, $r \cdot 1 = 0$ or $s \cdot 1 = 0$. By minimality of n, we have $r = n$ or $s = n$. So, n is a prime. So, $\mathbb{Z}_n$ is a field. So, R contains a field isomorphic of the field $\mathbb{Z}_n$.

If $char(L) = 0$ then $\varphi : \mathbb{Z} \longrightarrow R$ is injective. As we have seen in §21, there φ extends to a injective homomorphism $\psi : \mathbb{Q} \longrightarrow L$ such that the diagram



commutes and $r/s \mapsto (r \cdot 1)(s \cdot 1)^{-1}$.

The proof is complete. ∎

Definition 27.18. $\mathbb{Z}_p$ (with p prime) *and* $\mathbb{Q}$ *are called* **prime fields**.

27.4 Ideals in $F[x]$

Definition 27.19. Follwing are some definitions.

1. Suppose R is a commutative ring and $a \in R$. The ideal $Ra = \{ra : r \in R\}$ is called the **principal ideal** generated by a. In this textbook it is denoted by $\langle a \rangle$. (*In fact, Ra is more commonly used notation*).

2. An ideal N is called a **principal ideal** if $N = \langle a \rangle$ for some $a \in R$.

3. A commutative ring R is called a **Prinicipal Ideal Ring**, if evary ideal of R is principal.

Example 27.20 (27.22)**.** Every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z} = \langle n \rangle$. So $\mathbb{Z}$ is a principal ideal ring.

Question: How did we prove it? We used the Division Algorithm. The polynomial ring $F[x]$ over any files F, has a Division Algorithm. So, we have the following.

Theorem 27.21. Suppose F is a field. Then every ideal of $F[x]$ is principal. In other words, $F[x]$ is a principal ideal ring.

Proof. (*We will repeat the proof of (6.4) on subgroups of $\mathbb{Z}$.*) Let N be an ideal of $F[x]$. If $N = \{0\}$, then N is principal. Assume $N \neq \{0\}$. Consider the set,

$$S = \{n \in \mathbb{Z} : \exists\ f \in N\ \ni\ f \neq 0 \quad and \quad degree(f) = n\}.$$

Let

$$d = \min S, \quad let \quad g(x) \in N \quad \ni degree(f) = n.$$

If $d = 0$ then g is a nonzero constant in F. So, $N = F[x] = \langle 1 \rangle$ is principal. So, assume $d \geq 1$. We claim $N = F[x]g$. Since $g \in N$, we have $F[x]g \subseteq N$. To see the other inclusion, let $f(x) \in N$. Then, by division algorithm

$$f(x) = q(x)g(x) \quad for\ some \quad q(x), r(x) \in F[x]$$

$$with \quad r(x) = 0 \quad or \quad degree(r(x) < d = degree(g).$$

Note $r(x) \in N$. By minimality of $d = degree(g)$, we have $r(x) = 0$. So, $f(x) = q(x)g(x) \in F[x]g$. Therefore $N \subseteq F[x]g$.

Therefore, $N = F[x]g$ is principal. The proof is complete. ∎

Theorem 27.22. *Let F is a field and $p(x) \in F[x]$ be a nonzero non-constant polynomial. Then the principal ideal,*

$$\langle p(x) \rangle \quad \text{is maximal} \quad \Longleftrightarrow \quad p(x) \quad \text{is irreducible in} \quad F[x].$$

Proof. ($\Rightarrow$): Suppose $\langle p(x) \rangle$ is maximal, hence also is a prime ideal. Then $F[x]p(x) \neq F[x]$. So, $p(x) \notin F$. Now suppose $p(x) = f(x)g(x)$. We need to prove that either $f(x)$ of $g(x)$ is a unit. Since $f(x)g(x) \in \langle p(x) \rangle$, either $f(x) \in \langle p(x) \rangle$ of $g(x) \in \langle p(x) \rangle$. Assume $f(x) \in \langle p(x) \rangle$. So, either $f(x) = p(x)h(x)$ for some $h \in F[x]$. So, $p(x) = f(x)g(x) = p(x)h(x)g(x)$. Cancelling $h(x)g(x) = 1$. So, $g(x)$ is an unit. So, $p(x)$ is irreducible.

($\Leftarrow$): Suppose $p(x)$ is irreducible in $F[x]$. Suppose N is an ideal of $F[x]$ and $\langle p(x) \rangle \subseteq N$. Since $F[x]$ is principal ideal ring (see 27.21), $N = \langle g(x) \rangle$ for some $g(x) \in N$. So, $p(x) \in N = \langle g(x) \rangle$. Therefore $p(x) = g(x)f(x)$ for some $f(x)$. Since $p(x)$ is irreducible, either $g(x) \in F$ is a unit or $f(x) \in F$ is a unit. In the first case, $N = Fx$ and in the second case, $\langle p(x) \rangle = \langle g(x) \rangle = N$. So, $\langle p(x) \rangle$ is a maximal ideal. The proof is complete. ∎

Easy translation: For any commutative ring R and $r \in R$,

$$x \in \langle r \rangle \iff r|x \iff x \text{ is a multiple of } r.$$

In §23 we stated the following thoerem without proof.

Theorem 27.23. *Let $p(x)$ be an irreducible polinomial in $F[x]$. Then, for $r(x), s(x) \in F[x]$ we have*

$$p(x)|(r(x)s(x)) \quad \Longrightarrow \quad either \quad p(x)|r(x) \quad or \quad p(x)|s(x).$$

Proof. Suppose $p(x)|(r(x)s(x))$. Then $r(x)s(x) = q(x)p(x)$ for some $q(x) \in F[x]$. So, $r(x)s(x) \in \langle p(x) \rangle$. Since $\langle p(x) \rangle$ is a prime ideal (*in fact maximal ideal*) either $r(x) \in \langle p(x) \rangle$ or $s(x) \in \langle p(x) \rangle$. Assume $r(x) \in \langle p(x) \rangle$. Then $r(x) = p(x)h(x)$. So, $p(x)|r(x)$. The proof is complete. ∎

28 Göbner Bases for ideals

Skip.