

Last lecture

- A polynomial $f(x) \in R[x]$ is **primitive** if there is no irreducible element $p \in R$ such that $p|f(x)$.
- (Lemma 18.2) Suppose that $0 \neq f(x) \in R[x]$. Then there exists $p \in R$ and $q(x) \in R[x]$ such that $f(x) = p \cdot q(x)$ and $q(x)$ is primitive
- (Lemma 18.3) Suppose that $q(x)$ and $r(x)$ are primitive polynomials in $R[x]$. Then $q(x)r(x)$ is primitive.

This lecture

If R is a unique factorization domain then $R[x]$ is a unique factorization domain (continued) and the characteristic of a ring.

Polynomials in $F[x]$ and primitives

Recall that $F = F(R)$ is the field of fractions of R .

Lemma 19.1

Suppose that $f(x)$ is an irreducible polynomial in $F[x]$. Then there exists $\lambda \in F$ such that $\lambda f(x) \in R[x]$ and $\lambda f(x)$ is primitive and irreducible in $R[x]$.

Proof Every element of F can be written in the form $\frac{a}{b}$, for $a, b \in R$. Since R is a UFD we can write $\frac{a}{b} = \frac{a_1 \dots a_k}{b_1 \dots b_l}$, where $a_1, \dots, a_k, b_1, \dots, b_l$ are all irreducible. Moreover, since $\frac{c}{d} = \frac{uc}{ud}$ by Lemma 8.4, we can assume that a_i is not an associate of b_j for any i and j .

Let μ be the product of the denominators in the coefficients of $f(x)$
 $\implies 0 \neq \mu \in R$ and $\mu f(x) \in R[x]$.

By Lemma 18.2, $\mu f(x) = p \cdot q(x)$, where $p \in R$ and $q(x)$ is primitive

\implies Set $\lambda = \frac{\mu}{p} \in F$. Then $\lambda f(x) = q(x) \in R[x]$ is primitive.

Finally, $q(x)$ is irreducible in $R[x]$ because it is irreducible in $F[x]$, being an associate of $f(x)$. \square

Unique factorization in $R[x]$

Theorem 19.2

Suppose that R is a UFD. Then every non-zero element of $R[x]$ can be written in the form $up_1 \dots p_k q_1(x) \dots q_l(x)$, where u is a unit, p_1, \dots, p_k are irreducible in R and $q_1(x), \dots, q_l(x)$ are primitive in $R[x]$ and irreducible in $F[x]$. Moreover, this factorization is unique up to multiplication by units of R and reordering the factors.

Proof (Existence) Suppose that $f(x) \in R[x]$. By considering $f(x)$ as a polynomial in $F[x]$ we can write $f(x) = v f_1(x) \dots f_l(x)$, where v is a unit in $F[x]$ and $f_1(x), \dots, f_l(x)$ are irreducible in $F[x]$.

$\implies f(x) = v \lambda_1 \dots \lambda_l q_1(x) \dots q_l(x)$, where $\lambda_1, \dots, \lambda_l \in F$ and $q_1(x), \dots, q_l(x)$ are primitive irreducible polynomials in $R[x]$. Now, $f(x) \in R[x]$ and $q_1(x) \dots q_l(x)$ is a primitive polynomial in $R[x]$, by Lemma 18.3, so $v \lambda_1 \dots \lambda_l \in R$

$\implies v \lambda_1 \dots \lambda_l = up_1 \dots p_k$, where u is a unit and p_1, \dots, p_k are irreducible in R . Thus, $f(x)$ can be written in the required form.

Unique factorization in $R[x]$.../2

(Uniqueness)

Suppose that $up_1 \dots p_k q_1(x) \dots q_l(x) = vp'_1 \dots p'_m q'_1(x) \dots q'_n(x)$, where u and v are units in R , $p_1, \dots, p_k, p'_1, \dots, p'_m$ are irreducible elements of R and $q_1(x), \dots, q_l(x), q'_1(x), \dots, q'_n(x)$ are primitive polynomials in $R[x]$ which are irreducible in $F[x]$

$\implies q_1(x) \dots q_l(x)$ and $q'_1(x) \dots q'_n(x)$ are associates in $F[x]$, since any non-zero element of R is a unit

$\implies l = n$ and, after renumbering, $q_j(x)$ and $q'_j(x)$ are associates $\forall j$

$\implies up_1 \dots p_k$ and $vp'_1 \dots p'_m$ are associates in R since $q_1(x) \dots q_l(x)$ and $q'_1(x) \dots q'_l(x)$ are associates in $F[x]$ and primitive in $R[x]$ by Lemma 18.3

$\implies k = m$ and, after renumbering, p_i and p'_i are associates $\forall i$, since R is a unique factorization domain. \square

The irreducible elements of $R[x]$

Corollary 19.3

Suppose that R is a unique factorization domain and that F is the field of fractions of R . Then a polynomial $f(x) \in R[x]$ is irreducible if and only if either

- ① $f(x) \in R$ and $f(x)$ is irreducible in R , or,
- ② $f(x)$ is a primitive in $R[x]$ and irreducible in $F[x]$.

Proof Suppose that $f(x) \in R[x]$ is irreducible and write $f(x) = up_1 \dots p_k q_1(x)$ as in the Theorem 19.2

- \implies each p_i and $q_j(x)$ is either a unit or an associate of $f(x)$
- \implies either $f(x) = up_1$ or $f(x) = uq_1(x)$

For the converse, by definition, the irreducible elements of R and the primitive polynomials which are irreducible in $F[x]$ are irreducible in $R[x]$. □

More corollaries

Corollary 19.4

$\mathbb{Z}[x]$ is a unique factorization domain.

Corollary 19.5

Suppose that R is a unique factorization domain. Then $R[x_1, \dots, x_n]$ is a unique factorization domain for $n \geq 0$. In particular, $R[x]$ is a UFD.

Proof This follows from Theorem 19.2 by induction on n since $R[x_1, \dots, x_n] \cong (R[x_1, \dots, x_{n-1}])[x_n]$. □

Natural multiplication

Let R be any ring and define a map $*$: $\mathbb{Z} \times R \rightarrow R$; $(n, a) \mapsto n * a$ by

$$n * a = \begin{cases} \underbrace{a + a + \dots + a}_{n \text{ times}}, & \text{if } n > 0, \\ 0_R, & \text{if } n = 0, \\ \underbrace{-a - a - \dots - a}_{-n \text{ times}}, & \text{if } n < 0 \end{cases}$$

Properties of 'natural multiplication' $*$

Suppose that $m, n \in \mathbb{Z}$ and $a, b \in R$. Then

- $(m + n) * a = m * a + n * a$
- $m * (a + b) = m * a + m * b$
- $m * (n * a) = (mn) * a$

Remark This is actually saying that every ring R is a \mathbb{Z} -algebra.

Aside If S is a ring then an S -algebra is a ring A together with a ring homomorphism $\theta: S \rightarrow A$ which, in effect, allows us to multiply elements of A by elements of S : $s * a := \theta(s)a$.

The characteristic of a ring

Proposition 19.6

Suppose that R is a ring with one. Then the map $\chi: \mathbb{Z} \rightarrow R$; $n \mapsto n * 1_R$ is a ring homomorphism.

Proof Obvious from previous properties of natural multiplication! □

We have that $\ker \chi = c\mathbb{Z}$, for some $c \geq 0$, since \mathbb{Z} is a PID.

Definition 19.7

The **characteristic** of R is the unique non-negative integer $c = \text{Char } R$ such that $\ker \chi = c\mathbb{Z}$.

Remark By the first isomorphism theorem (theorem 7.3),

$$\text{im } \chi \cong \mathbb{Z}/c\mathbb{Z} \implies R \text{ has a subring isomorphic to } \mathbb{Z}/c\mathbb{Z}.$$

Remark By definition, the characteristic of R is the smallest non-negative integer such that $c * 1_R = \underbrace{1_R + \dots + 1_R}_{c \text{ times}} = 0_R$.

Hence, $n * 1_R = 0_R$ in $R \iff c | n$.