Intro to Algebra 2 W1-2

fat

February 23, 2024

Corollary 1. Assume that R is a UFD and F is its field of fractions. Let $f(x) \in R[x]$ be a polynomial s.t. $GCD(\text{coefficients of } f) = 1$. Then $f(x)$ is irreducible in $R[x] \Leftrightarrow f(x)$ is irreducible in $F[x]$.

Proof.

($\Rightarrow$) Gauss lemma.

($\Leftarrow$) (Note that this direction is not trivial. Think of R as $\mathbb{Z}$ and F as $\mathbb{Q}$. Take $f(x) = 2$.) Assume that $f(x)$ is irreducible in $F[x]$, but reducible in $R[x]$. Say $f(x) = a(x)b(x)$ in $R[x]$. Since $f(x)$ is irreducible in $F[x]$. We have $deg(a(x)) = 0$ or $deg(b(x)) = 0$. Suppose $deg(a(x)) = 0$, we have $a(x) = c$ for some nonunit $c \in R$. $\Rightarrow$ every coefficient of $f(x)$ is a multiple of c. This contradicts to the assumption that $GCD(\text{coefficient of } f) = 1$. $\Rightarrow f(x)$ is irreducible in $R[x]$.

$\square$

Theorem 1. Let R be an ID, then $R[x]$ is a UFD $\Leftrightarrow R$ is a UFD.

Proof.

($\Rightarrow$) has been explained.

($\Leftarrow$) We first prove that every nonzero, nonunit polynomial $f(x) \in R[x]$ can be factorized into a product of irreducibles in $R[x]$. Let F be the field of fractions. Let $f(x) = P_1(x) \dots P_k(x)$ be the factorization of $f(x)$ into irreducibles in $F[x]$. By Gauss's lemma, $\exists r_1, \dots, r_k \in F^\times$ s.t. the polynomials

$$p_j(x) \equiv r_j P_j(x)$$

are in $R[x]$ and $f(x) = p_1(x) \dots p_k(x)$. Let $d_j = GCD(\text{coefficients of } p_j(x))$ and $p'_j(x) = \frac{1}{d_j} p_j(x)$. Then $GCD(\text{coefficients of } p'_j(x)) = 1$. Now $p'_j(x)$ is a constant multiple of $p_j(x)$, which is irreducible in $F[x]$. Thus, $p'_j(x)$ is an irreducible polynomial in $F[x]$. By Corollary 1, $p'_j(x)$ is an irreducible polynomial in $R[x]$. Let $d = d_1 \dots d_k$ and $d = q_1 \dots q_n$ be the factorization of d into irreducibles in R. Note that q_j are irreducibles in $R[x]$ (since $R[x]^\times = R^\times$).

$$\Rightarrow f(x) = p_1(x) \dots p_k(x) = (d_1 p'_1(x)) \dots (d_k p'_k(x)) = q_1 \dots q_n p'_1(x) \dots p'_k(x)$$

is a factorization of $f(x)$ into irreducibles in $R[x]$.

Uniqueness of the factorization follows from the uniquenness of factorization in R and $F[x]$.

□

Corollary 2. If R is a UFD, then $R[x_1, \dots, x_n]$ is a UFD for any n.

9.4 Irreducibility Criteria

Proposition 1. Let F be a field and $f(x) \in F[x]$. Then $f(x)$ has a factor of degree 1 $\Leftrightarrow$ $f(x)$ has a root in F. In fact, for $a \in F$, $(x-a)|f(x) \Leftrightarrow f(a) = 0$.

Proposition 2. A polynomial of degree 2 or 3 is reducible in $F[x] \Leftrightarrow f(x)$ has a root in F.

Proposition 3. Let $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$. If $r/s \in \mathbb{Q}, (r,s) = 1$, is a root of $f(x)$, then $s|a_n, r|a_0$.

Proof.

We have $f(x) = (sx - r)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. By Gauss's lemma, $\exists c, d \in \mathbb{Q}^\times$ with $cd = 1$, s.t. $c(sx - r), dg(x) \in \mathbb{Z}[x]$. Now since $(s,r) = 1$, c must be an integer. Thus $c, d = \pm 1 \Rightarrow g(x) \in \mathbb{Z}[x]$. Comparing the leading coefficients in $f(x) = (sx - r)g(x)$, we see $s|a_n$. Comparing the constant term, we see that $r|a_0$. □

Proposition 4. Let R be an ID, $I \trianglelefteq R$, f a monic polynomial in $R[x]$. If $f \mod I$ (the image of f under the reduction homomorphism $R[x] \to (R/I)[x]$) cannot be factored into 2 polynomials of smaller degree in $(R/I)[x]$, then f is irreducible in $R[x]$.

Proof.

Assume $f = gh \in R[x]$. W.L.O.G. we may assume g, h are also monic. Consider the reduction modulo I. We have $\bar{f} = \bar{g}\bar{h}$. By assumption, $deg(\bar{g}) = 0$ or $deg(\bar{h}) = 0$. $\Rightarrow g = 1$ or $h = 1$. $\square$

Example 1.

$$f(x) = x^4 + 8x^3 + 12x^2 + 7x + 9 \in \mathbb{Z}[x]$$

From expericence, one could consider the reduction modulo 2. We can check that

$$x^4 + 8x^3 + 12x^2 + 7x + 9 \equiv x^4 + x + 1$$

is irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$. By Proposition 4, $x^4 + 8x^3 + 12x^2 + 7x + 9$ is irreducible in $\mathbb{Z}[x]$.

Example 2.

$$f(x, y) = x^2 + (3y + 1)x + (y^2 - 2y + 1) \in \mathbb{Q}[x, y](= \mathbb{Q}[y][x])$$

Consider $f \mod (y)$. We have $f(x, y) \equiv x^2+x+1$. Note that $\mathbb{Q}[x, y]/(y) \simeq \mathbb{Q}[x]$. Now x^2+x+1 is irreducible in $\mathbb{Q}[x] \Rightarrow f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proposition 5 (Eisenstein Criterion)**.** Let P be a prime ideal of an ID R. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Assume that $a_j \in P$ for $j = 0, \ldots, n-1$ and $a_0 \notin P^2$, then f is irreducible in $R[x]$.

Proof.

Consider the reduction modulo P. We have

$$f(x) \equiv x^n \mod (P) = P[x]$$

Thus if $f(x) = g(x)h(x)$, then

$$g(x)h(x) \equiv x^n \mod P$$

i.e. $\bar{g}\bar{h} = x^n$ in $(R/P)[x]$). Now P is a prime ideal and R is an ID. Over the ID R/P the only possible factorizations of x^n are $x^n x^k \cdot x^{n-k}$ for some $k, 0 \leq k \leq n$. Therefore

$$\begin{cases} \bar{g}(x) = x^k \\ \bar{h}(x) = x^{n-k} \end{cases} \quad \text{for some } k, 1 \leq k \leq n-k-1$$

$$\Rightarrow \begin{cases} \bar{g}(x) = x^k + b_k x^{k-1} + \ldots + b_0 \\ \bar{h}(x) = x^{n-k} + c^{n-k-1} x^{n-k-1} + \ldots + c_0 \end{cases} \quad \text{for some } b_j, c_j \in P$$

$\Rightarrow a_0 = b_0 c_0 \in P^2$ a contradiction. Therefore $f(x)$ cannot be factorized into a product 2 polynomials of smaller degree. $\Rightarrow$ The onlyl factorization of $f(x)$ in $R[x]$ is of the form $f(x) =$ (a constant) $\times$ (a polynomial). But since f is monic, the constant must be a unit. i.e., if we write f as a product of 2 polynomials, then one of the polynomials is a unit. $\Rightarrow f$ is irreducible in $R[x]$. $\square$

Example 3. 1. $x^4 + 8x^3 + 12x^2 + 4x + 2$ is irreducible in $\mathbb{Z}[x]$.

2. Let P be a prime. Let

$$f(x) = \prod_{k=1}^{p-1} (x - e^{2\pi i k/p}) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1$$

This is called the pth cyclotonic polynomial.

Claim. $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof.

Note that $f(x)$ is irreducible in $\mathbb{Z}[x] \Leftrightarrow g(x) = f(x+1)$ is irreducible in $\mathbb{Z}[x]$. Now

$$g(x) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{1}{x}(x^p + \binom{p}{1} x^{p-1} + \ldots + \binom{p}{p-1} x + 1 - 1)$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{p-2} x + \binom{p}{p-1}$$

Now $p | \binom{p}{j}$ for $j = 1, \ldots, p-1$. By the Eisenstein criterion, $g(x)$ is irreducible in $\mathbb{Z}[x] \Rightarrow f(x)$ is irreducible in $\mathbb{Z}[x]$. $\square$

Remark 1. It's possible that a polynomial in $\mathbb{Z}[x]$ is reducible modulo p for any prime p, but the polynomial is irreducible in $\mathbb{Z}[x]$. For example, let $f(x) = x^4 + 1$. We have

$$x^4 + 1 \equiv (x+1)^4 \mod 2$$

for $p \equiv \mod 8$, then since $(\mathbb{Z}/p\mathbb{Z})$ is cyclic, $\exists a \in \mathbb{Z}$ s.t. $a^4 \equiv -1 \mod p$. $\Rightarrow (x-a)|(x^4+1)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. Likewise, if $p \equiv 5 \mod 8$, $\exists a \in \mathbb{Z}$ s.t. $a^2 \equiv -1 \mod p$. $\Rightarrow (x^4+1) \equiv (x^2-a)(x^2+a) \mod p$. For $p \equiv 3 \mod 8$, we can show that $\exists a$ s.t. $a^2+2 \equiv 0 \mod p$. For $p \equiv 7 \mod 8$, $\exists a$ s.t. $a^{12} \equiv 2 \mod p$. $\Rightarrow x^4+1 \equiv (x^2-ax+1)(x^2+ax+1) \mod p$.