LESSON 5 - IRREDUCIBILITY CRITERIA

ERAN ASSAF

1. Introduction

Last lesson we have shown that polynomial rings over a field are UFD, and that the prime ideals correspond to monic irreducible polynomials. Today we will see some ways to find roots of polynomials and proving their irreducibility, will talk about irreducibility of polynomials and their factorization.

2. roots of polynomials

Proposition 1. *Let F be a field, $f(x) \in F[x]$. Then $f(x)$ has a* **factor** *of degree 1 if and only if $f(x)$ has a* **root** *in F, i.e. there is $\alpha \in F$ such that $f(\alpha) = 0$.*

Proof. Since F is a field, we may assume the factor $p(x) \mid f(x)$ is monic, hence of the form $p(x) = x - \alpha$ for some $\alpha \in F$. But then $p(\alpha) = 0$, so $f(\alpha) = 0$. Conversely, assume $f(\alpha) = 0$. Since $F[x]$ is Euclidean we can write $f(x) = q(x)(x - \alpha) + r(x)$ where $\deg r(x) < \deg(x - \alpha) = 1$ or $r(x) = 0$. It follows that $r(x) = r \in F$ is constant, and evaluating at α we obtain

$$0 = f(\alpha) = q(\alpha)(\alpha - \alpha) + r = 0 + r = r,$$

hence $r = 0$, and $x - \alpha \mid f(x)$. □

Corollary 2. *Let $f(x) \in F[x]$ be with $\deg f(x) \in \{2, 3\}$. Then $f(x)$ is reducible if and only if it has a root in F.*

Proof. $f(x)$ is reducible iff it has a linear factor, so by Proposition 1 we are done. □

Example 3. *The polynomial $f(x) = x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x] = (\mathbb{Z}/2\mathbb{Z})[x]$, since $f(0) = f(1) = 1$. Similarly, $x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.*

Proposition 4. *If the polynomial $f(x) \in F[x]$ has roots $\alpha_1, \ldots, \alpha_k$ (not necessarily distinct), then $f(x)$ has $(x - \alpha_1) \cdots (x - \alpha_k)$ as a factor. In particular, if $\deg f(x) = n$, then f has at most n roots in F, counting multiplicities.*

Proof. The first statement follows by induction from Proposition 1. Since linear factors are irreducible, the second statement follows since $F[x]$ is a UFD. □

Proposition 5. *Let $p(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, and let $r, s \in \mathbb{Z}$ be such that $(r, s) = 1$ and $p(r/s) = 0$. Then $r \mid a_0$ and $s \mid a_n$.*

Proof. By assumption

$$0 = p(r/s) = a_n(r/s)^n + \ldots + a_0.$$

Multiply by s^n to obtain

$$0 = a_n r^n + a_{n-1}r^{n-1}s + \ldots + a_1 r s^{n-1} + a_0 s^n.$$

Then $s \mid a_n r^n$, but $(r,s) = 1$ so $s \mid a_n$. Similarly, $r \mid a_0 s^n$, hence $r \mid a_0$. □

Example 6. *The polynomial $p(x) = x^3 - 3x - 1$ is irreducible in $\mathbb{Z}[x]$. Indeed, if it were reducible, it were also reducible in $\mathbb{Q}[x]$. However, by Corollary 2, that means it would have a root in $\mathbb{Q}$. Write $r/s \in \mathbb{Q}$ in lowest terms. By Proposition 5, we must have $r, s \mid 1$, hence $r/s = \pm 1$, but $p(1) = -3, p(-1) = 1$ so $p(x)$ does not have a rational root.*

Proposition 7. *Let I be a proper ideal in the integral domain R, and let $p(x)$ be a non-constant monic polynomial in $R[x]$. Let $\widetilde{\pi} : R[x] \to (R/I)[x]$ be the natural map. If $\widetilde{\pi}(p(x))$ is irreducible, then so is $p(x)$.*

Proof. Assume that $p(x) = a(x)b(x)$ for some $a(x), b(x) \in R[x]$. Then, as $p(x)$ is monic, we may assume $a(x)$ and $b(x)$ are monic. Since $\widetilde{\pi}(p(x)) = \widetilde{\pi}(a(x))\widetilde{\pi}(b(x))$ and $\widetilde{\pi}(p(x))$ is irreducible, w.l.o.g. we may assume $\widetilde{\pi}(b(x)) \in (R/I)[x]^\times$. But $b(x)$ is monic, hence $\deg b(x) = 0$, showing that $b(x) \in R^\times$, hence $p(x)$ is irreducible. □

Example 8. *The polynomials $x^2 + x + 1$ and $x^3 + x + 1$ are irreducible in $\mathbb{Z}[x]$ since they are irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$.*

Example 9. *The polynomial $x^4 - 22x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ as can be checked directly However, as we shall prove, it is reducible modulo every prime. (exercise!).*

3. Eisenstein's Criterion

The last proposition we have proved in the last lesson gave us a good tool to show irreducibility of polynomials in $R[x]$ by reducing the coefficients modulo an ideal I. A special well-known case of that idea is the following criterion.

Theorem 10 (Eisenstein's Criterion)**.** *Let P be a prime ideal of the integral domain R, and let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be a polynomial in $R[x]$. Suppose $a_{n-1}, \ldots, a_1, a_0 \in P$ and $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.*

Proof. Assume, on the contrary, that $f(x) = g(x)h(x)$ in $R[x]$. Let $\pi : R \to R/P$ be the natural projection, and $\widetilde{\pi} : R[x] \to (R/P)[x]$. Then, by assumption

$$x^n = \widetilde{\pi}(f(x)) = \widetilde{\pi}(g(x))\widetilde{\pi}(h(x)) =: \overline{g}(x)\overline{h}(x).$$

Since P is a prime ideal, R/P is an integral domain, hence $(x) \subseteq (R/P)[x]$ is a prime ideal. It follows that either $\overline{g}(x) \in (x)^n$ or $\overline{h}(x) \in (x)^n$ or both $\overline{g}(x) \in (x)$ and $\overline{h}(x) \in (x)$. Since R/P is an integral domain, $x^n \mid \overline{g}(x)$ implies $\deg g(x) \geq n$, hence $\deg g(x) = n$ and $h(x) \in R$ is constant. Since f is monic, looking at the leading term we obtain $h \in R^\times$. Similarly, if $x^n \mid \overline{h}(x)$, then g is constant. Therefore, if both g, h are nonconstant, we must have $\overline{g}(0) = \overline{h}(0) = 0$, whence

$$a_0 = f(0) = g(0)h(0) \in P^2,$$

contradiction. □

Pedestrian approach. Assume $f(x) = g(x)h(x)$, where $g(x) = \sum_{i=0}^{m} b_i x^i$ and $h(x) = \sum_{j=0}^{k} c_j x^j$. Since f is monic, we may assume g and h are monic, hence $b_m = c_k = 1$, and $m + k = n$. Evaluating at 0, we see that $b_0 c_0 = g(0)h(0) = f(0) = a_0 \in P$. Since P is a prime, it follows that either $b_0 \in P$ or $c_0 \in P$. Assume without loss of generality that $b_0 \in P$. Since P is a prime ideal, it is proper, and $1 = b_m \notin P$. Therefore, there exists a minimal index $i \in \{1, \ldots, m\}$ such that $b_i \notin P$. If $i \leq n - 1$, then from $f(x) = g(x)h(x)$ we obtain

$$\sum_{j=0}^{\min(i,k)} c_j b_{i-j} = a_i \in P,$$

but by minimality of i, for all $j > 0$, we have $b_{i-j} \in P$, hence $c_j b_{i-j} \in P$ so that $c_0 b_i \in P$. But $b_i \notin P$ and P is prime, hence $c_0 \in P$. However, then $a_0 = b_0 c_0 \in P^2$, contradiction. Since $m \leq n$, it then follows that $i = m = n$, hence that $k = 0$, and $h(x) = 1$, showing that f is irreducible. □

Example 11. *The polynomial $x^n - p \in \mathbb{Z}[x]$ is irreducible for all primes p and all $n \geq 2$. In particular, we obtain another proof that $\sqrt[n]{p} \notin \mathbb{Q}$.*

Example 12. *The polynomial $f(x) = x^4 + 1 \in \mathbb{Z}[x]$ is irreducible. Indeed, $f(x)$ is irreducible iff $g(x) = f(x + 1)$ is irreducible. But*

$$g(x) = f(x + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2,$$

so by Eisenstein criterion with $p = 2$, $g(x)$ is irreducible, hence so is $f(x)$.

Example 13. *Consider the polynomial*

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Then

$$\Phi_p(x + 1) = \frac{(x + 1)^p - 1}{x} = x^{p-1} + px^{p-2} + \ldots + \frac{p(p-1)}{2}x + p \in \mathbb{Z}[x]$$

with all the coefficients but the first divisible by p. Hence, by Eisenstein's criterion with p, $\Phi_p(x)$ is irreducible in $\mathbb{Z}[x]$.

Example 14. *Let $R = \mathbb{Q}[t]$, and consider $x^n - t \in R[x]$. The ideal (t) is prime in R since $R/(t) = \mathbb{Q}[t]/(t) \simeq \mathbb{Q}$ is an integral domain. Eisenstein's criterion for the ideal (t) of R applies to show that $x^n - t$ is irreducible in $R[x]$. ($\mathbb{Q}$ can be replace by any integral domain).*

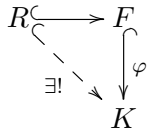
4. Gauss' Lemma

We have seen ways to prove irreducibility of polynomials by reduction of coefficients. However, if the coefficient ring is a field, e.g. in $\mathbb{Q}[x]$, there are no nontrivial ideals to reduce by! However, there is something else we can do to prove irreducibility of polynomials in $F[x]$, when F is a field - we can "clear denominators". More precisely, if $f(x) =$

$g(x)h(x) \in \mathbb{Q}[x]$, there exist some $a, b \in \mathbb{Z}$ such that $ag(x), bh(x) \in \mathbb{Z}[x]$, and so $abf(x) = (ag(x))(bh(x))$ in $\mathbb{Z}[x]$. Therefore, it suffices to prove irreducibility of $f(x)$ in $\mathbb{Z}[x]$. This is the content of Gauss' Lemma.

In order to state it in a more general setting, we need to formalize the relation between $\mathbb{Q}$ and $\mathbb{Z}$, and we recall that $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.

Definition 15. *Let R be an integral domain. The* **field of fractions** *of R, F is the field containing R satisfying the following universal property - any embedding $\varphi : R \hookrightarrow K$ to a field K, factors uniquely through F.*



Example 16. *For $\mathbb{Z}$ this is $\mathbb{Q}$, for the polynomial ring $F[t]$, this is $F(t)$, the function field in one variable over F, consisting of rational functions.*

Theorem 17 (Gauss' Lemma)**.** *Let R be a UFD with field of fractions F, and let $f(x) \in R[x]$. If $f(x)$ is reducible in $F[x]$ then $f(x)$ is reducible in $R[x]$. More precisely if $f(x) = g(x)h(x)$ for some nonconstant polynomials $g(x), h(x) \in F[x]$, there are $r, s \in F$ such that $G(x) = rg(x), H(x) = sh(x) \in R[x]$, and $f(x) = G(x)H(x)$.*

Proof. Clearing denominators, we obtain $df(x) = \tilde{g}(x)\tilde{h}(x)$ for some $0 \neq d \in R$ and $\tilde{g}(x) = ag(x), \tilde{h}(x) = bh(x) \in R[x]$. If $d \in R^\times$, we can set $r = d^{-1}a, s = d^{-1}b$ and we are done. If not, since R is a UFD, we can write d as a product of irreducibles $d = p_1 \cdots p_n$. Since p_1 is irreducible, the ideal (p_1) is prime, so $p_1R[x]$ is prime in $R[x]$ and $(R/p_1R)[x]$ is an integral domain. Reducing modulo p_1 we obtain

$$0 = \overline{df(x)} = \overline{\tilde{g}(x)} \cdot \overline{\tilde{h}(x)},$$

hence w.l.o.g. $\tilde{g}(x) \in p_1R[x]$. But then $p_1^{-1}g(x) \in R[x]$. Therefore, replacing $\tilde{g}(x)$ by $p_1^{-1}\tilde{g}(x)$ we obtain

$$p_2 \cdots p_n f(x) = \tilde{g}(x)\tilde{h}(x).$$

We finish by induction on n, the number of irreducible factors of d. □

Example 18. *Since $x^2 = (2x) \cdot \left(\frac{1}{2}x\right)$ in $\mathbb{Q}[x]$, it follows that x^2 is reducible in $\mathbb{Z}[x]$.*

Example 19. *The polynomial $7x \in \mathbb{Z}[x]$ is not irreducible, since 7 is not a unit, although it is irreducible in $\mathbb{Q}[x]$.*

Corollary 20. *Let R be a UFD, with field of fraction F. Let $p(x) = a_nx^n + \ldots + a_1x + a_0 \in R[x]$ be such that $\gcd(a_0, \ldots, a_n) = 1$. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $F[x]$, it is irreducible in $R[x]$.*

Proof. If $p(x) = g(x)h(x)$ in $R[x]$, from the assumption it follows that neither g nor h are constant, hence it is also a factorization in $F[x]$. The converse is Gauss's Lemma. □

5. SUMMARY

Today we talked about way to determine irreducibility of polynomials. We have seen the powerful Eisenstein criterion, and Gauss's Lemma, which together allow us to determine irreducibility of polynomials over $\mathbb{Q}[x]$ in many cases.

6. Appendix: Factorization of polynomials

There is an algorithm to factor polynomials in $\mathbb{Q}[x]$. To see this, note that by clearing denominators it's enough to consider monic polynomials in $\mathbb{Z}[x]$. From the fundamental theorem of algebra (which we will prove later on, but has many proofs), $f(x)$ splits completely in $\mathbb{C}[x]$, i.e. $f(x) = \prod_i (x - \alpha_i)$ for some $\alpha_i \in \mathbb{C}$. From the equation $0 = f(\alpha) = \alpha^n + \ldots + a_0$ it follows that $|\alpha|$ is bounded. Indeed, if $|\alpha| > 1$ then

$$|\alpha|^n = |\alpha^n| = \left|\sum_{i=0}^{n-1} a_i \alpha^i\right| \leq \sum_{i=0}^{n-1} |a_i||\alpha|^i \leq n \max_i |a_i||\alpha|^{n-1},$$

showing that $|\alpha| \leq n \max_i |a_i|$.

If $g(x)$ is a monic factor of $f(x)$ then its roots are some of the α_i, and its coefficients are symmetric polynomials in its roots. Therefore, we can bound the absolute value of its coefficients in terms of the degree and the coefficients of $f(x)$. Indeed, if $g(x) = x^d + b_{d-1}x^{d-1} + \ldots + b_0$ then $|b_j| \leq \binom{n}{j} n^j \max |a_i|^j$. Since the coefficients are integers, this reduces the problem to a finite search.

Of course, there are much faster methods. The one commonly used is the Berlekamp-Zassenhaus algorithm, which uses the Chinese Remainder Theorem. Indeed, given the bounds on the size of the coefficients, we can find primes $p_1, \ldots, p_m$ whose product is larger, and then by the CRT it suffices to know the value of each coefficient modulo each of the p_i, i.e. the factorization modulo each of the primes. One factors the polynomial over each $\mathbb{F}_p$ (there is an efficient method of doing that), and then one can search for factorizations over $\mathbb{Z}[x]$ that have the correct form modulo each p_i.