Lecture 13: Irreducible Polynomials

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Irreducible Polynomials

- If R is an integral domain $\Rightarrow R[x]$ is an integral domain.
- If F is a field $\Rightarrow F[x]$ is not a field, but $F[x]$ is a Euclidean domain. $U(F[x]) = F^*$ and the associates of a nonconstant $f(x)$ is $uf(x)$, where $u \in F^*$.
  $F[x]$ is a ED with Euclidean norm $\upsilon(f(x)) = \deg f(x)$.
- If R is a PID $\Rightarrow R[x]$ may not be a PID.
  $\mathbb{Z}$ is a PID, but $\mathbb{Z}[x]$ is not a PID. In particular, in $\mathbb{Z}[x]$

$$\begin{aligned} \langle 2, x\rangle &= \{2f(x) + xg(x) \mid f, g \in \mathbb{Z}[x]\} \\ &= \{2a_0 + a_1 x + \cdots + a_r x^r \in \mathbb{Z}[x] \mid r \geq 0\} \end{aligned}$$

  which does not include 1, so $\langle 2, x\rangle$ is not a PID.
- If R **is a UFD** $\Rightarrow R[x]$ **is a UFD.**

Irreducible Polynomials

From the definition of irreducible element, we have the following:

Definition

Let R be a commutative ring with unit. A nonzero and nonunit polynomial $f(x) \in R[x]$ is **irreducible polynomial** if

$$f(x) = g(x)\,h(x) \Rightarrow \text{either } g(x) \text{ or } h(x) \text{ is a unit.}$$

If $f(x) \in R[x]$ is not irreducible, then $f(x)$ is **reducible** over R.

Remark: A nonconstant polynomial $f(x) \in F[x]$ is **irreducible polynomial** in $F[x]$ (or irreducible over F) if $f(x)$ can not be expressed as a product of two polynomials $g(x), h(x) \in F[x]$ such that $\deg g(x) < \deg f(x)$, $\deg h(x) < \deg f(x)$.

Examples:

1. $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, since there does not exist $a, b, c, d \in \mathbb{Q}$ such that

$$x^2 - 2 = (ax + b)(cx + d).$$

But $x^2 - 2$ is reducible in $\mathbb{R}[x]$, since

$$x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$$

where $x - \sqrt{2}, x + \sqrt{2} \in \mathbb{R}[x]$.

2. $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, since there does not exist $a, b, c, d \in \mathbb{R}$ such that

$$x^2 + 1 = (ax + b)(cx + d).$$

But $x^2 + 1$ is reducible in $\mathbb{C}[x]$, since

$$x^2 + 1 = (x + i)(x - i).$$

3. Let $a \neq 0$, $ax + b \in F[x]$ is irreducible over F.

Now we give some useful information about the irreducibility of polynomials over $\mathbb{C}$ and $\mathbb{R}$.

- **Fundamental Theorem of Algebra:** Every nonconstant polynomial in $\mathbb{C}[x]$ has a zero in $\mathbb{C}$.
- Every irreducible polynomials over $\mathbb{C}$ has degree 1. ($\mathbb{C}$ is algebraically closed.)
  If $f(x) \in \mathbb{C}[x]$ has degree n, then
  $$f(x) = a(x - a_1)(x - a_2)\ldots(x - a_n).$$
- If α is a root of a polynomial in $\mathbb{R}[x]$, then $\overline{\alpha}$ is also a root.
- Every irreducible polynomials over $\mathbb{R}$ has degree 1 or 2.

Irreducibility tests

It may be difficult to determine whether a given polynomial is irreducible or not. So for testing irreducibility, it would be useful to give some criteria.

- If $f(x) \in F[x]$ has a root in F, then $f(x)$ is reducible.
  Because if $f(x) \in F[x]$ has a root $\mathbf{a}$ in F means that $f(x)$ has a degree 1 factor; that is, $x - \mathbf{a}$ is a factor.
- If $f(x) \in F[x]$ has no root in F, then $f(x)$ may be irreducible or not!
  But if we know that the degree of $f(x)$ is 2 or 3, then it is quarantee that $f(x)$ is irreducible.

Irreducibility of quadratic and cubic polynomials

Theorem

Let $f(x)$ be a polynomial in $F[x]$ with degree 2 or 3. Then

$$f(x) \text{ is reducible over } F \Leftrightarrow f(x) \text{ has a zero in } F.$$

Example: $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ is irreducible over $\mathbb{Z}_5$.
Since $f(0) = 2$, $f(1) = 1$, $f(2) = 1$, $f(3) = 3$, $f(4) = 3$ which are all nonzero.

Remark: If degree of $f(x) \in F[x]$ is not 2 or 3, the theorem may not be true.

Example: $x^4 - 5x^2 + 6$ has no root in $\mathbb{Q}$, but it is reducible

$$x^4 - 5x^2 + 6 = \left(x^2 - 2\right)\left(x^2 - 3\right).$$

The following theorem helps to find all rational roots of polynomial in $\mathbb{Z}[x]$, if it exists. If no such a root exist, it might still possible to find a way to factor it!

Theorem (Rational Root Test)

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. Any rational number $\frac{r}{s}$ that is a root of $f(x)$ must have $r \mid a_0$ and $s \mid a_n$.

Example: $2x+2$ is irreducible in $\mathbb{Q}[x]$. Note that $2x+2=2(x+1)$ where 2 is a unit in $\mathbb{Q}[x]$. Since 2 is a unit in $\mathbb{Z}[x]$, $2x+2$ is **reducible** in $\mathbb{Z}[x]$.

Definition

Let R be UFD. A nonconstant polynomial $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ in $R[x]$ is called a **primitive** polynomial if $\gcd(a_0,a_1,\ldots,a_n)$ is a unit. Here, gcd of coefficients is called the **content** of $f(x)$.

Irreducibility over Q

Theorem (Gauss's Lemma)

Product of two primitive polynomial is also primitive.

By the help of the Gauss's Lemma we have the followings:

Theorem

Let R be UFD, $\mathbf{Q}$ be a quotient field of R and $f(x)$ be a nonconstant **primitive** *polynomial in $R[x]$.*

$$f(x) \text{ is irreducible in } R[x] \Leftrightarrow f(x) \text{ is irreducible in } \mathbf{Q}[x].$$

In particular,

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

Irreducibility over Q

Theorem (Eisenstein Criterion)

Let $p \in \mathbb{Z}$ be a prime. If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ with

1. $p \mid a_0, p \mid a_1, \ldots p \mid a_{n-1}$
2. $p \nmid a_n$
3. $p^2 \nmid a_0$.

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example: $f(x) = x^5 + 3x^3 - 3x + 6$ is irreducible in $\mathbb{Q}[x]$ by E.K. with $p = 3$.

Irreducibility over Q

Theorem (Mod p Criterion)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and $\overline{f}(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0} \in \mathbb{Z}_p[x]$ be polynomials degree n. If $\overline{f}(x)$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example: Show that $f(x) = x^3 + 7x + 16$ is irreducible in $\mathbb{Q}[x]$.
For $p = 5$, we get $x^3 + \overline{2}x + \overline{1} \in \mathbb{Z}_5[x]$. Since it has degree 3 and has no root in $\mathbb{Z}_5$, it is irreducible in $\mathbb{Z}_5[x]$. Hence $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Irreducible Polynomials

Example: Let $f(x) = x^4 + 1 \in \mathbb{Z}[x]$.

- The possible rational roots are ± 1. Since $f(\pm 1) \neq 0$, it has no degree 1 factors.
  We need to chech if it has degree 2 factors. That is, check if there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{aligned} x^4 + 1 &= \left(x^2 + ax + b\right)\left(x^2 + cx + d\right) \\ &= x^4 + (a + c)\,x^3 + (d + ac + b)\,x^2 + (bc + ad)\,x + bd \end{aligned}$$

  By compairing the coefficients, we have $b = d = -1$ and $a = -c$. So $ac - 2 = 0$ implies $a^2 = -2$, which contradicts $a \in \mathbb{Z}$.
  Thus $f(x) = x^4 + 1$ is irreducible over $\mathbb{Q}$.
- Since

$$x^4 + 1 = \left(x^2 - \sqrt{2}x + 1\right)\left(x^2 + \sqrt{2}x + d\right),$$

  it is not irreducible over $\mathbb{R}$ and $\mathbb{C}$.

Remark: In group theory, we used the division algorithm in $\mathbb{Z}$ to prove that a subgroup of a cyclic group is also cyclic, which shows that $\mathbb{Z}$ is a PID. On the other hand, the division algorithm in $F[x]$ is used to show that $F[x]$ is a PID.

- Every ideal of $F[x]$ is principal.
- Every maximal ideal is prime in $F[x]$.

Theorem

Let $p(x) \in F[x]$. Then

$$p(x) \text{ is irreducible over } F \Leftrightarrow F[x]/\langle p(x)\rangle \text{ is a field}$$

So $\langle p(x)\rangle$ is a maximal ideal.

Example: $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field since x^2+1 is irreducible over $\mathbb{Z}_3$.

Uniqueness of Factorization of F[x]

Basic Goal: To show that any nonconstant polynomial $f(x)$ in $F[x]$ has a zero in some field E containing F.

1. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$
2. Let E be the field $F[x]/\langle p(x)\rangle$
3. Show that no two different elements of F are in the same coset of $F[x]/\langle p(x)\rangle$
4. Consider F to be isomorphic to a subfield of E
5. For the evaluation homomorphism $\phi_\alpha : F[x] \to E$, we have $\phi_\alpha(f(x)) = 0$. Thus α is a zero of $f(x)$ in E.