

Last lecture

- If $f(x) \in F[x]$ and $\alpha \in F$ then α is a **zero** or **root** of $f(x)$ if $f(\alpha) = 0$ in F .
- (Lemma 22.2) If $f(x) \in F[x]$ and $\alpha \in F$ then α is a **zero** of $f(x)$ if and only if $(x - \alpha) | f(x)$.
- (Proposition 21.3) Suppose that $\alpha_1, \dots, \alpha_k$ are the distinct zeros of the polynomial $f(x) \in F[x]$ with multiplicities m_1, \dots, m_k , respectively. Then $f(x) = (x - \alpha_1)^{m_1} \dots (x - \alpha_k)^{m_k} g(x)$, where $g(x) \in F[x]$ has no zeros in F .
- (Corollary 22.4) The number of zeros, counted with multiplicity, of a polynomial over a field is at most the degree of the polynomial.
- (Corollary 22.6) A polynomial in $\mathbb{Z}[x]$ factorizes as a polynomial in $\mathbb{Q}[x]$ if and only if it factorizes in $\mathbb{Z}[x]$.

This lecture

The rational roots theorem and Eisenstein's irreducibility criterion.

The rational roots theorem

Theorem 23.1 (The rational roots theorem)

Suppose that $f(x) = f_0 + f_1x + \cdots + f_dx^d \in \mathbb{Z}[x]$, with $f_d \neq 0$. Then $\alpha \in \mathbb{Q}$ is a zero of $f(x)$ only if there exist $m, n \in \mathbb{Z}$ such that $m|f_0$, $n|f_d$ and $\alpha = \frac{m}{n}$.

Proof Suppose that $\alpha = \frac{m}{n}$ is a zero of $f(x)$.

$\implies (x - \alpha) | f(x)$ by Lemma 22.2

$\implies f_0 + f_1x + \cdots + f_dx^d = (x - \alpha)(g_0 + g_1x + \cdots + g_{d-e}x^{d-e})$,
for some rational numbers $g_0, \dots, g_{d-e} \in \mathbb{Q}$

Hence, by Corollary 22.6 there exist $\lambda \in \mathbb{Q}$ such that $\lambda(x - \alpha) \in \mathbb{Z}[x]$ and $\frac{1}{\lambda}(g_0 + g_1x + \cdots + g_{d-e}x^{d-e}) \in \mathbb{Z}[x]$.

Write $\lambda(x - \alpha) = nx - m$ ($\implies \alpha = \frac{m}{n}$)

and $\frac{1}{\lambda}(g_0 + g_1x + \cdots + g_{d-e}x^{d-e}) = h_0 + \cdots + h_{d-1}x^{d-1} \in \mathbb{Z}[x]$

$\implies f(x) = (nx - m)(h_0 + \cdots + h_{d-1}x^{d-1}) = -mh_0 + \cdots + nh_{d-1}x^d$

$\implies f_0 = -mh_0$ and $f_d = nh_{d-1}$, for $m, n, h_0, h_{d-1} \in \mathbb{Z}$

$\implies m|f_0$ and $n|f_d$ as required. □

The rational roots theorem in action

Remark This gives an algorithm for finding all of the zeros of a polynomial over \mathbb{Q} . In more detail, if $f(x) \in \mathbb{Q}[x]$ pick $\lambda \in \mathbb{Z}$ so that $p(x) = \lambda f(x) \in \mathbb{Z}[x]$. Then $\frac{m}{n} \in \mathbb{Q}$ is a root of $f(x)$ if and only if m divides the constant term of $p(x)$ and n divides the leading coefficient of $p(x)$ and there are only a finite number of such choices.

Examples

- ① $f(x) = x^2 - 2$ is irreducible over \mathbb{Q} since $f(\pm 1) = -1 \neq 0$
and $f(\pm 2) = 2 \neq 0$

$\implies f(x)$ has no zeros in \mathbb{Q}

$\implies f(x)$ is irreducible over \mathbb{Q}

- ② $g(x) = x^{2d} + x^{2d-1} + \dots + x + 1$ has no zeros in \mathbb{Q} for any $d \geq 0$ since $g(\pm 1) = \pm 1$

Note that this does **not** imply that $g(x)$ is irreducible over \mathbb{Q} !

Being irreducible and having no zeros are not the same!

- $f(x)$ has no zeros $\iff f(x)$ has no **linear** factors
- $f(x)$ is irreducible $\iff f(x)$ has no **non-trivial** factors.

Changing base rings

Proposition 23.2

Let R and S be commutative rings and suppose that $\theta : R \rightarrow S$ is a ring homomorphism. Then the map $\Theta : R[x] \rightarrow S[y]$ given by

$$\Theta\left(\sum_{i=0}^d f_i x^i\right) = \sum_{i=0}^d \theta(f_i) y^i$$

is a ring homomorphism.

Proof We need to check that Θ respects addition and multiplication. This follows directly from the definitions because θ is a ring homomorphism (and so respects addition and multiplication). \square

Remark Implicitly, we have already used this result to embed $R[x]$ into $F[x]$, where $F = F(R)$ is the field of fractions of R .

The main case where we want to apply this result is to compare polynomials in $\mathbb{Z}[x]$ with polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$, when p is prime.

Eisenstein's irreducibility criterion

Theorem 23.3 (Eisenstein's irreducibility criterion)

Suppose that $f(x) = f_0 + f_1x + \cdots + f_dx^d \in \mathbb{Z}[x]$ and that there exists a prime $p \in \mathbb{Z}$ such that

① $p|f_0, p|f_1, \dots, p|f_{d-1}$

② $p \nmid f_d$

③ $p^2 \nmid f_0$

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

Remark Note that $f_d \neq 0$ since $p \nmid f_d$.

Proof Suppose by way of contradiction that $f(x)$ is reducible in $\mathbb{Q}[x]$. By Corollary 22.6, we can write $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ $\implies \deg f(x) = \deg g(x) + \deg h(x)$

Let $d_g = \deg g(x)$ and $d_h = \deg h(x)$
 $\implies d = d_g + d_h$ and $0 < d_g, d_h < d$.

By Proposition 23.2 the quotient map $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ gives rise to a ring homomorphism $\mathbb{Z}[x] \rightarrow (\mathbb{Z}/p\mathbb{Z})[x]$; $a(x) = \sum_i a_i x^i \mapsto \overline{a(x)} = \sum_i \overline{a_i} x^i$.
 $\implies \overline{f(x)} = \overline{g(x)h(x)}$, so $\overline{f(x)}$ is reducible over $\mathbb{Z}/p\mathbb{Z}$.

Eisenstein's irreducibility criterion.../2

Now, $\overline{f(x)} = \overline{f_d}x^d$ since $p \nmid f_d$ and $p|f_i$ for $0 \leq i < d$.

Write $g(x) = g_0 + g_1x + \dots + g_{d_g}x^{d_g}$ and $h(x) = h_0 + h_1x + \dots + h_{d_h}x^{d_h}$

$\implies \overline{g(x)} = \overline{g_{d_g}}x^{d_g}$ and $\overline{h(x)} = \overline{h_{d_h}}x^{d_h}$ since $(\mathbb{Z}/p\mathbb{Z})[x]$ is a UFD.

$\implies \overline{f_d}x^d = (\overline{g_0} + \overline{g_1}x + \dots + \overline{g_{d_g}}x^{d_g})(\overline{h_0} + \overline{h_1}x + \dots + \overline{h_{d_h}}x^{d_h})$

Therefore, $p|g_0$ and $p|h_0$ since $\overline{g(x)} = \overline{g_{d_g}}x^{d_g}$ and $\overline{h(x)} = \overline{h_{d_h}}x^{d_h}$

$\implies p^2|f_0 = g_0h_0$ since $p|g_0$ and $p|h_0$ (note that $d_g, d_h \geq 1$)

This is a contradiction as $p^2 \nmid f_0$ by assumption!

$\implies f(x)$ is irreducible □

Examples

① $x^2 - 2$ is irreducible over \mathbb{Q} .

② $x^5 - 2$ is irreducible over $\mathbb{Q} \implies \sqrt[5]{2}$ is irrational

Note that, saying that $x^5 - 2$ is irreducible over \mathbb{Q} is a much stronger statement than simply saying that $\sqrt[5]{2}$ is irrational.

③ $\frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3}$ is irreducible over \mathbb{Q} (take $p = 3$)

④ $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over \mathbb{Q}

Trick $f(x)$ is irreducible $\iff f(x+1)$ is irreducible.