A.5 · Polynomials and field extensions

Original classroom teaching; not an official form or score predictor

Polynomials and field extensions

- Use the division algorithm and the factor theorem.
- Decide whether a polynomial is an **irreducible polynomial** 不可约多项式 over a given field.
- Find extension degrees with the tower law.
- Find minimal polynomials and build finite fields.

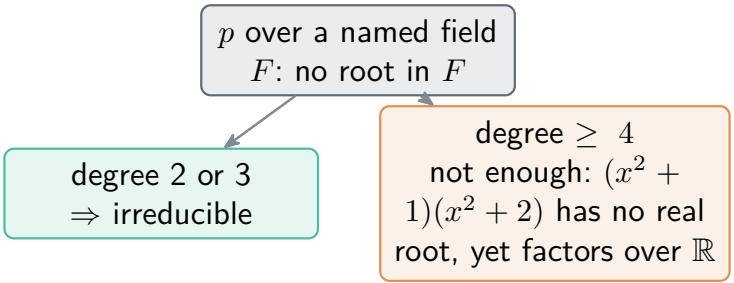
Division and roots

- For polynomials over a field, $f = qg + r$ with $\deg r < \deg g$.
- Factor theorem: a is a root of f exactly when $(x - a)$ divides f.
- A polynomial of degree n over a field has at most n roots.

Irreducibility

- Degree 2 or 3: irreducible exactly when there is no root in the field.
- Degree 4 or more: no root is not enough. $(x^2+1)(x^2+2)$ has no real root but factors.
- Rational root test: a rational root p/q of an integer polynomial has p dividing the constant term and q dividing the leading coefficient.
- Eisenstein: if a prime p divides every coefficient except the leading one, and p^2 does not divide the constant term, the polynomial is irreducible over $\mathbb{Q}$.

Figure: Irreducibility



- The root test works only up to degree 3.
- Match each part of the diagram to the text.

Extensions and degrees

- $[L : K]$ is the dimension of L as a vector space over K.
- If α has minimal polynomial of degree n over K, then $[K(\alpha) : K] = n$.
- Tower law: $[M : K] = [M : L][L : K]$.
- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, since $x^3 - 2$ is irreducible by Eisenstein.

Finite fields

- If f is irreducible of degree n over $\mathbb{F}_p$, then $\mathbb{F}_p[x]/(f)$ is a field with p^n elements.
- There is exactly one field of each prime-power order, up to isomorphism, and none of any other order.
- The nonzero elements of a finite field form a cyclic group.

Figure: Finite fields

$F_2[\alpha]$, with $\alpha^2 = \alpha + 1$: all nonzero elements invertible

×	1	α	α + 1
1	1	α	α + 1
α	α	α + 1	1
α + 1	α + 1	1	α

- Every nonzero element of $F_2[\alpha]$ has an inverse, so it is a field with four elements
- Match each part of the diagram to the text.

Worked example: a field with four elements

- $x^2 + x + 1$ is 1 at both $x = 0$ and $x = 1$, so it has no root in $\mathbb{F}_2$. Having degree 2, it is irreducible, and the quotient is a field.
- Its elements are $0, 1, \alpha, 1 + \alpha$, with $\alpha^2 = \alpha + 1$.
- $\alpha(\alpha + 1) = \alpha^2 + \alpha = 1$, so $\alpha^{-1} = \alpha + 1$. This field is not $\mathbb{Z}/4\mathbb{Z}$, which has the zero divisor 2.

Worked example: a degree-4 extension

- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, so the tower law gives $2 \times 2 = 4$.
- Let $x = \sqrt{2} + \sqrt{3}$. Then $x^2 = 5 + 2\sqrt{6}$, so $(x^2 - 5)^2 = 24$ and $x^4 - 10x^2 + 1 = 0$.
- $\sqrt{2} + \sqrt{3}$ generates the whole degree-4 field, so this quartic is its minimal polynomial.

Common errors

- Calling a polynomial irreducible without naming the field.
- Using the no-root test for degree 4 or more.
- Assuming a field of order 4 is $\mathbb{Z}/4\mathbb{Z}$.

Common errors (2)

- Multiplying degrees in the tower law without checking each step's degree.
- Applying Eisenstein's criterion with p^2 dividing the constant term.

Key terms

- **extension degree**: The dimension of an extension field as a vector space over its base field.
- **irreducible polynomial**: A polynomial of positive degree that cannot be written as a product of polynomials of lower positive degree over the given field.

Check yourself

- Is $x^3 + x + 1$ irreducible over $\mathbb{F}_2$?
- Is there a field with 6 elements?
- What is $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$?