

A.5 · Polynomials and field extensions

GRE · GRE Subject Test · GRE Mathematics

Scope and prerequisites

Undergraduate GRE preparation. Local objectives within the reviewed ETS scope; this is original teaching, not an official test or score predictor.

Prerequisites: Polynomial division, fields and vector-space dimension.

- Test polynomial irreducibility over the specified field
- Construct small finite fields from irreducible polynomials
- Use extension degrees and the tower law
- Use cyclotomic roots and coefficient relations to compute sums and products

irreducible polynomial : A positive-degree polynomial with no factorisation into smaller positive degrees over the stated field.

extension degree : The dimension of an extension field as a vector space over its base field.

Choose and justify a method

A polynomial is irreducible over a field if it has positive degree and no factorisation into polynomials of smaller positive degrees there. A quadratic or cubic is irreducible exactly when it has no root in that field. This root test alone fails for degree four or higher; for instance $(x^2+1)(x^2+2)$ has no real root but is reducible over $\mathbb{R}$. Always name the base field.

The quotient $F[x]/(p)$ is a field when p is irreducible. Reduce powers using $p(\alpha)=0$, where α is the residue class of x . If F has q elements and p has degree d , the quotient has q^d elements represented by polynomials of degree below d . $\mathbb{Z}/4\mathbb{Z}$ has four elements but has zero divisors, so it is not the field with four elements.

Over F_2 , $p(x)=x^2+x+1$ has values 1 at both 0 and 1 and is irreducible. In its quotient $\alpha^2=\alpha+1$ because subtraction equals addition in characteristic two. The four elements are 0, 1, α , $\alpha+1$. All three nonzero elements must be units; compute their products rather than treating α as an ordinary real number.

For nested finite-degree fields K inside L inside M , the tower law gives $[M:K]=[M:L][L:K]$. The degree of an algebraic element is the degree of its minimal polynomial. A finite extension of degree two does not contain an element of degree three over the base field. Over $\mathbb{Q}$, $\sqrt{2}$ has degree two; adjoining $\sqrt{3}$ as well produces a degree-four extension, since $\sqrt{3}$ is not in $\mathbb{Q}(\sqrt{2})$. Over $\mathbb{C}$, primitive n th roots of unity have exact order n and are the roots of the cyclotomic polynomial Φ_n . For $n=10$, divide x^5+1 by $x+1$ to exclude the order-two root -1 : $\Phi_{10}=x^4-x^3+x^2-x+1$. Vieta's formulas give sum 1 and product 1 of its four primitive roots. Do not sum all tenth roots, or assume every nontrivial tenth root is primitive; a root's order must be

checked. For a monic degree d polynomial, product of its roots is $(-1)^d$ times the constant coefficient.

Worked reasoning

In $\mathbb{F}_2[\alpha]$ with $\alpha^2+\alpha+1=0$, multiply $\alpha(\alpha+1) = \alpha^2 + \alpha = (\alpha+1) + \alpha = 1$. Thus $\alpha^{-1}=\alpha+1$. Also $\alpha^3=1$ and α is not 1, so its multiplicative order is 3. This produces a field of four elements. By contrast $2 \cdot 2=0$ in $\mathbb{Z}/4\mathbb{Z}$, proving that quotient is not a field.

$\mathbb{F}_2[\alpha]$, with $\alpha^2 = \alpha + 1$: all nonzero elements invertible

$\times$	1	α	$\alpha + 1$
1	1	α	$\alpha + 1$
α	α	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	1	α

Original course illustration; its values belong to the worked example, not the later practice.

Conditions and counterexamples

Polynomial reducibility changes with the coefficient field. The polynomial x^2-2 is irreducible over $\mathbb{Q}$ but splits over $\mathbb{R}$.

Guided application

Construct $\mathbb{F}_2[x]/(x^2 + x + 1)$. List its elements and find the inverse of the residue $\alpha = [x]$.

■ Worked solution

The quadratic takes value one at both elements of $\mathbb{F}_2$, so it has no root and is irreducible. Its quotient is a field. Division leaves a representative of degree below two: $0, 1, \alpha, 1 + \alpha$. The relation is $\alpha^2 = \alpha + 1$ in characteristic two. Consequently $\alpha(\alpha + 1) = \alpha^2 + \alpha = 1$, so $\alpha^{-1} = \alpha + 1$. This is not $\mathbb{Z}/4\mathbb{Z}$, which has a nonzero zero divisor.

Independent transfer

Is $x^4 + 4$ irreducible over $\mathbb{Q}$? Does the absence of rational roots answer that question? Can a degree-two extension of $\mathbb{Q}$ contain a root of an irreducible cubic over $\mathbb{Q}$?

■ Check after attempting

Direct multiplication gives $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$, so it is reducible over $\mathbb{Q}$ despite having no real, hence no rational, roots. The no-root test characterises irreducibility only for degree two or three over a field. If an irreducible cubic root β belonged to a degree-two extension L , then $\mathbb{Q} \subset \mathbb{Q}(\beta) \subset L$ and the tower law would make 3 divide 2. This is impossible. The conclusion uses irreducibility, not merely a cubic equation.