11.1 Polynomials and field extensions

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

KEY WORDS irreducible polynomial • extension degree

Objective

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.

Original public practice. Marking guidance is authored locally. Use the topic reference for prerequisites and full theorem statements.

1 Key knowledge and worked examples

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.

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 R. Always name the base field.

In F2[alpha] with alpha^2+alpha+1=0, multiply alpha(alpha+1) = alpha^2 + alpha = (alpha+1) + alpha = 1. Thus alpha$\widehat{}$−1=alpha+1. Also alpha^3=1 and alpha is not 1, so its multiplicative order is 3. This produces a field of four elements. By contrast $2 \cdot 2=0$ in Z/4Z, proving that quotient is not a field.

$F_2[\alpha]$, 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

2 Practice

2.1 Which polynomial is irreducible over F2? [1]

- **A** x^2
- **B** x^2+1
- **C** x^2+x
- **D** x^2+x+1
- **E** x^3+x^2

2.2 If [L:K]=3 and [M:L]=2, what is [M:K]? [1]

- **A** 1
- **B** 2
- **C** 3
- **D** 5
- **E** 6

2.3 Construct $\mathbb{F}_2[x]/(x^2 + x + 1)$. List its elements and find the inverse of the residue $\alpha = [x]$. [4]

3 Exam-style questions

3.1 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 $\mathbb{Q}$? [4]

Solutions

2.1 D. The quadratic x^2+x+1 has no root among 0 and 1. The others factor as $x \cdot x$, $(x+1)^2$, $x(x+1)$ and $x^2(x+1)$, respectively, over F2. The four rejected polynomials factor respectively as x times x, (x+1) squared, x(x+1), and x squared times (x+1) in characteristic two.

2.2 E. The tower law multiplies finite degrees, giving 2 times 3=6. One, two and three omit a nontrivial extension factor; five adds degrees instead of multiplying them.

2.3 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.

3.1 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.

Local four-mark guidance for each written task: choose and justify the method; carry through the reasoning; give every requested result; check the relevant restriction, hypothesis or boundary case. These are classroom marks, not GRE scoring.