18.702 May 10, 2008

Quiz 3

All questions are of equal value. Please show your work.

1. Determine the number of irreducible monic polynomials of degree 3 *over the field* $\mathbb{F}_5$.

Let $q = 5^3 = 125$. One part of the main theoreem about finite fields asserts that $x^q - x$ is a product of all monic irreducible polynomials whose degrees divide 3. There are 5 monic polynomials of degree 1, and therefore $120/3 = 40$ irreducible monic polynomials of degree 3.

2. Let α *be a complex root of the polynomial* x^3+x+1. *Determine the irreducible polynomial for* $\beta = \alpha^2$ *over* $\mathbb{Q}$.

We write the relation $\alpha^3 + \alpha + 1 = 0$ in the form $\alpha^3 = -\alpha - 1$. Then

$$\beta^2 = \alpha^4 = \alpha(-\alpha - 1) = -\beta - \alpha,$$

$$\beta^3 = \alpha^6 = (-\alpha - 1)^2 = \beta + 2\alpha + 1.$$

Eliminating α from these two relations: $\beta^3 + 2\beta^2 = -\beta + 1 = 0$.
So β is a root of x^3+2x^2+x-1. This polynomial is irreducible modulo 2, hence irreducible.

3. Write the symmetric polynomial $u_1^3 + u_2^3 + u_3^3$ *in three variables as a polynomial in the elementary symmetric functions* s_1, s_2, s_3.

$u_1^3 + u_2^3 + u_3^3 = s_1^3 - 3s_1s_2 + 3s_3$.

4. Let K *be a splitting field of the polynomial* $x^5 - 2$ *over* $\mathbb{Q}$. *Determine the degree* $[K : \mathbb{Q}]$.

The splitting field is generated over $\mathbb{Q}$ by $\alpha = \sqrt[5]{2}$ and $\zeta = e^{2\pi i/5}$. Since $x^5 - 2$ is irreducible, α has degree 5 over $\mathbb{Q}$. We also know that the irreducible polyniomial for ζ over $\mathbb{Q}$ is $x^4 + x^3 + x^2 + x + 1$, so ζ has degree 4 over $\mathbb{Q}$. Since 4 and 5 are relatively prime, $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 20$.

5. You are given that the Galois group of a Galois extension K *of* F *is the dihedral group* D_5. *Determine the number of intermediate fields* $F \subset L \subset K$, *and their degrees over* F.

The intermediate fields are the fixed fields of the subgroups of $G = D_5$. There is a cyclic subgroup H of order 5, and all elements not in this subgroup are reflections of order 2. So G contains five subgroups, say $U_1, ..., U_5$, of order 2.

The degree $[K : K^H]$ is five, so $[K^H : F] = 2$. Similarly, $[K^{U_i} : F] = 5$. These are the six intermediate fields other than F and K.