Homework

Frederick Robinson

17 May 2010

1 Chapter 14 Section 2

1.1 Problem 5

1.1.1 Question

Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p$, $a \neq 0$.

1.1.2 Answer

By the previous exercise we know that if θ is the real $\sqrt[p]{2}$ and ζ a principle pth root of unity then all elements of the group are $\sigma_{(m,n)}$ ($0 \leq n \leq p-1$, $1 \leq m \leq p-1$) where

$$\sigma_{(m,n)} : \begin{cases} \zeta \mapsto \zeta^m \\ \theta \mapsto \theta\zeta^n \end{cases}$$

I claim that the correspondence between this group and the one provided defined by

$$\varphi : \sigma_{(m,n)} \mapsto \begin{pmatrix} m & n \\ 0 & 1 \end{pmatrix}$$

is an isomorphism.

Proof. This correspondence is clearly bijective, so it suffices to show that it is a homomorphism. We compute

$$\sigma_{(m_1,n_1)} \cdot \sigma_{(m_2,n_2)}(\zeta) = \zeta^{m_1 m_2}$$

$$\begin{aligned} \sigma_{(m_1,n_1)} \cdot \sigma_{(m_2,n_2)}(\theta) &= \sigma_{(m_1,n_1)}(\theta\zeta^{n_2}) \\ &= \theta\zeta^{n_1}\zeta^{m_1 n_2} \\ &= \theta\zeta^{n_1 + m_1 n_2}. \end{aligned}$$

Moreover, we can compute

$$\begin{pmatrix} m_1 & n_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} m_2 & n_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} m_1 m_2 & n_1 + m_1 n_2 \\ 0 & 1 \end{pmatrix}.$$

Thus, $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$ and φ is a homomorphism as claimed. □

1.2 Problem 13

1.2.1 Question

Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then the roots of the cubic are real.

1.2.2 Answer

Proof. Let $f \in \mathbb{Q}[x]$ be a cubic and suppose that f has a complex root. The Galois group has a subgroup generated by complex conjugation since it has a complex root. This subgroup is $\mathbb{Z}/2\mathbb{Z}$ which is not a subgroup of $\mathbb{Z}/3\mathbb{Z}$ so the Galois group of f is not $\mathbb{Z}/3\mathbb{Z}$. □

2 Chapter 14 Section 3

2.1 Problem 1

2.1.1 Question

Factor $x^8 - x$ into irreducibles in $\mathbb{Z}[x]$ and in $\mathbb{F}_2[x]$.

2.1.2 Answer

In $\mathbb{Z}[x]$ we can factor $f(x) = x^8 - x$ as $f(x) = x(x-1)\left(1 + x + x^2 + x^3 + x^4 + x^5 + x^6\right)$. The degree 6 polynomial in this factorization is irreducible since $f(x+1) = 7 + 21x + 35x^2 + 35x^3 + 21x^4 + 7x^5 + x^6$ is Eisenstein (with $p = 7$).

By Proposition 18 we have in $\mathbb{F}_2$ that f is the product of all the distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree d where d runs through all divisors of 3. In particular this means that f is the product of all distinct irreducible polynomials of degrees 1,3 in $\mathbb{F}_2$. Hence

$$f(x) = x(x-1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

We can check that

$$x(x-1)(x^3 + x^2 + 1)(x^3 + x + 1) = x^8 + 2x^5 - 2x^4 - x$$

which indeed reduces mod 2 to $x^8 - x$ as claimed.

2.2 Problem 3

2.2.1 Question

Prove that an algebraically closed field must be infinite.

2.2.2 Answer

Proof. Fix some finite field. By Proposition 15 this field is just $\mathbb{F}_{p^n}$ for some prime p, integer $n \geq 1$. However, from the book (page 588) we have

$$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$$

and so we may conclude that the algebraic closure of $\mathbb{F}_p$, a subfield of our given field is nonfinite. Hence, $\mathbb{F}_{p^n}$ must have nofinite algebraic closure. □

2.3 Problem 5

2.3.1 Question

Exhibit an explicit isomorphism between the splitting fields of $x^3 - x + 1$ and $x^3 - x - 1$ over $\mathbb{F}_3$.

2.3.2 Answer

We first verify that $x + 1$ is a root of $f_2(x) = x^3 - x - 1$ in $\mathbb{F}_3[x]/(f_2)$ since

$$\begin{aligned} f_2(x+1) &= (1+x)^3 - x - 2 \\ &= x^3 + 3x^2 + 2x - 1 \\ &= x^3 + 2x - 1 \\ &= x^3 - x - 1 \\ &= 0 \end{aligned}$$

So, the homomorphism of splitting fields $\varphi : \mathbb{F}_3[x]/(f_1) \to \mathbb{F}_3[x]/(f_2)$ defined by

$$\varphi : x \mapsto x + 1$$

is an isomorphism.

2.4 Problem 7

2.4.1 Question

Prove that one of $2, 3$ or 6 is a square in $\mathbb{F}_p$ for every prime p. Conclude that the polynomial

$$x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6)$$

has a root modulo p for every prime p but has no root in $\mathbb{Z}$.

2.4.2 Answer

Proof. Let x be a generator of the field $\mathbb{F}_p$, and assume that neither 2, nor 3 are squares in $\mathbb{F}_p$. Then, since $\langle x \rangle = \mathbb{F}_p$ we know that $x^l = 2$ and $x^k = 3$ for some $k, l \in \mathbb{Z}$. Moreover, both k, and l must be odd, else they would be squares as $(x^{k/2})^2$ or $(x^{l/2})^2$. Hence, $x^l x^k = x^{k+l} = 6$ and since k and l are both odd $(x^{(k+l)/2})^2 = 6$ and 6 is a square. □

Since one of 2, 3, or 6 is a square in $\mathbb{F}_p$ one of the corresponding polynomials $(x^2 - 2)$, $(x^2 - 3)$, or $(x^2 - 6)$ has a root. Hence, the product of these always has a root.

2.5 Problem 10

2.5.1 Question

Prove that n divides $\varphi(p^n - 1)$. [Observe that $\varphi(p^n - 1)$ is the order of the group of automorphisms of a cyclic group of order $p^n - 1$.]

2.5.2 Answer

Proof. First note that

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

which in particular implies that $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$. However, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a subgroup of the group of automorphism on the additive group $\mathbb{F}_{p^n}^+$. Thus since $\varphi(p^n - 1)$ is the order of the group of automorphisms of a cyclic group of order $p^n - 1$ we have by Lagrange's Theorem

$$m = \frac{\varphi(p^n - 1)}{|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|}$$

for $m \in \mathbb{N}$ as desired. □