Homework

Frederick Robinson

28 May 2010

1 Chapter 14 Section 6

1.1 Problem 3

1.1.1 Question

Prove that for any $a, b \in \mathbb{F}_{p^n}$ that if $x^3 + ax + b$ is irreducible then $-4a^3 - 27b^2$ is a square in $\mathbb{F}_{p^n}$.

1.1.2 Answer

We have from the book that the discriminant for a cubic is

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

However, in the notation of the book we have $a = 0$, $b = a$, $c = b$. Substituting reveals that in our case

$$D = -4a^3 - 27b^2.$$

Since the Galois group corresponding to a finite extension of a finite field is cyclic we know that the Galois group in this case is the Cyclic group of order 3, and that the discriminant must be a square in the base field.

1.2 Problem 11

1.2.1 Question

Let F be an extension of $\mathbb{Q}$ of degree 4 that is not Galois over $\mathbb{Q}$. Prove that the Galois closure of F has Galois group either S_4, A_4 or the dihedral group D_8 of order 8. Prove that the Galois group is dihedral if and only if F contains a quadratic extension of $\mathbb{Q}$

1.2.2 Answer

Say that $E/\mathbb{Q} = \bar{F}$. For some root $\alpha \in F$ we can say $F = \mathbb{Q}(\alpha)$, so E is the splitting field of teh minimal polynomial of α. Since this is a degree 4 polynomial we know in particular that $G = \mathrm{Gal}(E/\mathbb{Q})$ is a subgroup of S_4.

Since E has a subfield that is 4th degree in $\mathbb{Q}$, G has a subgroup of index 4. We know that $|G| > 4$ since F is not Galois over $\mathbb{Q}$. Therefore $|G| = 8, 12$, or 24.

In the case that $|G| = 8$ we have $G = D_8$, the only group of order 8 that has a subgroup which is not normal and therefore corresponds to F. In the case that $|G| = 24$, G is just S_4 itself. If $|G| = 12$ it is just the only index 2 subgroup of S_4, A_4.

F contains a quadratic extension of $\mathbb{Q}$ if and only if each index 4 subgroup of G is contained in an index 2 subgroup. Both S_4, and A_4 fail this condition, but each element of D_8 having order 2 is contained in a subgroup of order 4.

1.3 Problem 17

1.3.1 Question

Find the Galois group of $x^4 - 7$ over $\mathbb{Q}$ explicitly as a permutation group on the roots.

1.3.2 Answer

Denote the roots of $f(x) = x^4 - 7$ by

$$\pm\alpha = \pm\sqrt[4]{7} \quad \pm\beta = \pm i\sqrt[4]{7}.$$

It is easy to verify that the Klein 4-group generated by

$$\sigma = (-\alpha\ \alpha) \quad \tau = (-\beta\ \beta)$$

is a subgroup of the Galois group. Moreover, since the resolvent cubic is $h(x) = x^3 + 28$ which splits into a linear and a quadratic term this is the entire Galois group.

1.4 Problem 19

1.4.1 Question

Let $f(x)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[x]$ with discriminant D. Let K denote the splitting field of $f(x)$, viewed as a subfield of the complex numbers $\mathbb{C}$.

1. Prove that $\mathbb{Q}(\sqrt{D}) \subset K$.
2. Let τ denote complex conjugation and let τ_K denote the restriction of complex conjugation to K. Prove that τ_K is an element of $\mathrm{Gal}(K/\mathbb{Q})$ of order 1 or 2 depending on whether every element of K is real or not.
3. Prove that if $D < 0$ then K cannot be cyclic of degree 4 over $\mathbb{Q}$ (i.e., $\mathrm{Gal}(K/\mathbb{Q})$ cannot be a cyclic group of order 4).
4. Prove generally that $\mathbb{Q}(\sqrt{D})$ for squarefree $D < 0$ is not a subfield of a cyclic quartic field (cf. also Exercise 19 of Section 7).

1.4.2 Answer

1. *Proof.*

$$\sqrt{D} = \prod_{i<j}(x_i - x_j)$$

for x_i a root of f. However every root of F is in K. Hence $\sqrt{D} \in K \Rightarrow \mathbb{Q}(\sqrt{D}) \subset K$ as claimed. □

2. *Proof.* If K is real then clearly τ_K is just the identity permutation, and thus of order 1. In the case that there is some root of K which is not real τ_K is a member of the Galois group since complex conjugation is an automorphism of $\mathbb{C}$ which is surjective in the restriction (as roots are in conjugate pairs). Moreover it must be of order 2 since the unresticted automorphism has this property and there is, by assumption at least one element of K which is not taken by complex conjugation to itself. □

3. *Proof.* Suppose towards a contradiction that $D < 0$ with K cyclic of order 4. Then, since K is cyclic and f is irreducible $K = F(\alpha)$ for any root α of f.

Since $D < 0$ f cannot have a real root. Thus, all roots have nonzero imaginary part. Since roots occur in complex conjugate pairs we may compute

$$\begin{aligned}
\sqrt{D} &= (x-\bar{x})(x-y)(x-\bar{y})(\bar{x}-y)(\bar{x}-\bar{y})(y-\bar{y}) \\
&= (x-\bar{x})(y-\bar{y})(x-y)\overline{(x-y)}(x-\bar{y})\overline{(x-\bar{y})} \\
&= 4\Re x \Re y (x-y)\overline{(x-y)}(x-\bar{y})\overline{(x-\bar{y})} \\
&= 4\Re x \Re y \left|x-y\right|^2 \left|x-\bar{y}\right|^2
\end{aligned}$$

but this is real, contradicting our assumption that $D < 0$. □

4. A degree 4 cyclic group has only one proper, nontrivial subgroup. That is the index 2 subgroup. By the fundamental theorem then there is only one quadratic extension of $\mathbb{Q}$ in a cyclic quartic field K. The only possibility is that this is $\mathbb{Q}(\sqrt{D})$. So, we conclude that if $\mathbb{Q}(\sqrt{E}) \subset K$ for E square free we have $E = D$ (by the previous part $D \geqslant 0$)

1.5 Problem 20

1.5.1 Question

Determine the Galois group of $(x^3 - 2)(x^3 - 3)$ over $\mathbb{Q}$. Determine all the subfields which contain $\mathbb{Q}(\rho)$ where ρ is a primitive 3^{rd} root of unity.

1.5.2 Answer

The Galois group restricted to just the roots of one of the irreducible factors must be a subgroup of the Galois group corresponding to that irreducible factors.

Any member of the Galois group must therefore be expressible as a product of the following

$$\sigma_2 : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \qquad \tau_2 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

$$\sigma_3 : \begin{cases} \sqrt[3]{3} \mapsto \rho\sqrt[3]{3} \\ \rho \mapsto \rho \end{cases} \qquad \tau_3 : \begin{cases} \sqrt[3]{3} \mapsto \sqrt[3]{3} \\ \rho \mapsto \rho^2 \end{cases}$$

and the Galois group is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The subfields containing ρ are the subfields fixed by automorphisms which fix ρ. There are nine such automorphisms. Namely the ones generated by σ_2, σ_3.

1.6 Problem 33

1.6.1 Question

1. Prove that the discriminant of the cyclotomic polynomial $\Phi_p(x)$ of the p^{th} roots of unity for an odd prime p is $(-1)^{(p-1)/2}p^{p-2}$. [One approach: use Exercise 5 of the previous section together with the determinant form for the discriminant in terms of the power sums p_i.]

2. Prove that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) \subset \mathbb{Q}(\zeta_p)$ for p an odd prime. (Cf. also Exercise 11 of Section 7.)

1.6.2 Answer

Proof. We have from exercise 32 that

$$D = (-1)^{n(n-1)/2}R(f, f')$$

given

$$R(f, f') = \prod_{i=1}^{n} f'(\alpha_i)$$

Since in this particular instance we know that

$$\Phi_p = x^{p-1} + x^{p-2} + \cdots + 1$$

we have in particular

$$\Phi_p' = (p-1)x^{p-2} + (p-2)x^{p-3} + \cdots + 1.$$

Evaluating the product we get

$$\prod_{i=1}^{n} f'(\alpha_i) = i^{-1+2n-n^2}p^{p-2}$$

by employing the result of exercise 5 from the previous section. □

The second statement follows from part 1 of the previous exercise.