MORE HOMEWORK SOLUTIONS
MATH 114

Problem set 8.

1. Let F be the splitting field of the polynomial $x^4 + 25$ over $\mathbb{Q}$. List all subfields in F and the corresponding subgroups in the Galois group.

Solution. As we proved in class $(F/\mathbb{Q}) = 4$. The Galois group G is the Klein subgroup of S_4, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note that F contains i and $\sqrt{5}$, each subgroup of G of index 2 corresponds to a subfield of degree 2. There are 3 such subfiels $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{5}\right)$ and $\mathbb{Q}\left(\sqrt{-5}\right)$. The trivial subgroup of G corresponds to F and G corresponds to $\mathbb{Q}$.

2. Prove that the Galois group of $x^4 - 5$ is isomorphic to D_4. Hint: prove that the degree of the splitting field is 8, then recall that the Galois group is a subgroup of S_4.

Solution. By Eisenstein criterion $x^4 - 5$ is irreducible. Let F be a splitting field, then we have the following chain of extensions

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, i) = F,$$

where α is a real root of $x^4 - 5$. Thus,

$$(F/\mathbb{Q}) = (\mathbb{Q}(\alpha, i)/\mathbb{Q}(\alpha))(\mathbb{Q}(\alpha)/\mathbb{Q}) = 2 \times 4 = 8,$$

the Galois group G is a subgroup of S_4 of order 8. Since G is a Sylow subgroup of S_4 and all such subgroups are conjugate, hence isomorphic, we obtain G is isomorphic to D_4.

3. Prove that the Galois group of $x^4 + 5x^2 + 5$ over $\mathbb{Q}$ is cyclic of order 4. Hint: use the formula for the roots.

Solution. The polynomial is irreducible by Eisenstein criterion. The roots can be found from the formulae

$$\alpha_{1,2} = \left(\frac{-5 \pm \sqrt{5}}{2}\right)^{1/2}, \ \alpha_{3,4} = -\alpha_{1,2}.$$

First, we prove that the splitting field has degree 4. Indeed

$$\alpha_1\alpha_2 = \sqrt{5} = 2\alpha_1^2 + 5,$$

hence

$$\alpha_2 = 2\alpha_1 + \frac{5}{\alpha_1} \in \mathbb{Q}(\alpha_1), \ \alpha_3 = -\alpha_1 \in \mathbb{Q}(\alpha_1), \ \alpha_4 = -\alpha_2 \in \mathbb{Q}(\alpha_1).$$

Date: April 4, 2006.

The Galois group G is a subgroup of S_4 of order 4. There exists $s \in G$ such that $s(\alpha_1) = \alpha_2$, then

$$s\left(\sqrt{5}\right) = 2s(\alpha_1)^2 + 5 = 2\alpha_2^2 + 5 = -\sqrt{5}.$$

Then

$$s(\alpha_2) = s\left(\frac{\sqrt{5}}{\alpha_1}\right) = \frac{-\sqrt{5}}{\alpha_2} = -\alpha_1 = \alpha_3,\ s(\alpha_3) = s(-\alpha_1) = -\alpha_2 = \alpha_4.$$

The order of s is 4, therefore G is isomorphic to $\mathbb{Z}_4$.

4. Let $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$, $b \neq 0$.

(a) Prove that if α is a root of $f(x)$, then $-\alpha$ and $\frac{\sqrt{b}}{\alpha}$ are also roots.

(b) Prove that the degree of the splitting field is 1,2,4 or 8.

(c) Prove that the Galois group is isomorphic to $\{1\}$, $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$ or D_4.

Solution. (a) can be done by direct check. Indeed,

$$\left(\frac{\sqrt{b}}{\alpha}\right)^4 + a\left(\frac{\sqrt{b}}{\alpha}\right)^2 + b = \frac{b^2 + ab\alpha^2 + b\alpha^4}{\alpha^4} = \frac{b + a\alpha^2 + \alpha^4}{b\alpha^4} = 0.$$

To show (b) denote the splitting filed by F. Then $\sqrt{b} \in F$ and $\mathbb{Q}\left(\alpha, \sqrt{b}\right)$ clearly contains all roots of $x^4 + ax^2 + b$. $(\mathbb{Q}(\alpha)/\mathbb{Q}) = 1, 2$ or 4 (this degree can not be 3, because the polynomial could not have only one rational root), $\left(\mathbb{Q}\left(\alpha, \sqrt{b}\right)/\mathbb{Q}(\alpha)\right) =$ 1 or 2. Hence

$$\left(\mathbb{Q}\left(\alpha, \sqrt{b}\right)/\mathbb{Q}\right) = (\mathbb{Q}(\alpha)/\mathbb{Q})\left(\left(\mathbb{Q}\left(\alpha, \sqrt{b}\right)/\mathbb{Q}(\alpha)\right) = 1, 2, 4 \text{ or } 8.$$

Finally, for (c) note that the order of the Galos group is the same as the degree of the splitting field. Thus, if the order is 2, the group is $\mathbb{Z}_2$, if the order is 4 the group is either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$. If the order of the Galois group is 8, the group is isomorphic to D_4, because it is a subgroup of S_4 (see the previous problem).

5. For a cubic polynomial $f(x) = x^3 + ax + b$ the discriminant is given by the formula

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

Assume that a and b are real numbers. Prove that D is negative if and only if $f(x)$ has exactly one real root.

Solution. Use

$$D = (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_1 - \alpha_3)^2,$$

where $\alpha_1, \alpha_2, \alpha_3$ are the roots. If all 3 roots are real, then D is a square of a real number. Hence $D \geq 0$. Assume that α_1, α_2 are complex conjugate, α_3 is real. Write

$$\alpha_1 = a + bi, \alpha_2 = a - bi, \alpha_3 = c.$$

Then
$$D = (bi)^2 (a-c-bi)^2 (a-c+bi)^2 = -b^2 \left((a-c)^2 + b^2\right)^2 < 0.$$

6. Assume that $f(x) = g(x)h(x)$ for some separable polynomials $f(x), g(x), h(x) \in F[x]$. Denote by E_f, E_g and E_h the splitting fields of the polynomials $f(x), g(x)$ and $h(x)$ respectively. Let
$$(E_f/F) = (E_g/F)(E_h/F).$$
Prove that the Galois group of $f(x)$ is isomorphic to the direct product of the Galois groups of $g(x)$ and $h(x)$.

Solution. Let $G = \operatorname{Aut}_F E_f$ be the Galois group of $f(x), K = \operatorname{Aut}_{E_g} E, H = \operatorname{Aut}_{E_h} E$. Since E_g and E_h are normal extensions of F, K and H are normal subgroups of G and by fundamental theorem of Galois theory
$$\operatorname{Aut}_F E_h \cong G/H, \operatorname{Aut}_F E_g \cong G/K.$$
Consider the subgroup $U = K \cap H \subset G$. Note that U fixes every element of E_g and E_h, but $E_g E_h = E_f$, therefore $K \cap H = \{1\}$. Consider the restriction map $r \colon G \to \operatorname{Aut}_F E_h$, the kernel of r is H. Therefore $r : K \to \operatorname{Aut}_F E_h$ is injective as $K \cap H = \{1\}$. Note that r is surjective because
$$|\operatorname{Aut}_F E_h| = (E_h/F) = \frac{(E_f/F)}{(E_g/F)} = \frac{|G|}{|G/K|} = |K|.$$
Thus, r is an isomorphism and we obtain $K \cong \operatorname{Aut}_F E_h$. Similarly $H \cong \operatorname{Aut}_F E_g$. Finally $G = KH$, because $|KH| = |K||H| = |G|$.

Problem set # 9

1. Let $n = p$, or $2p$ where p is a prime number. Prove that the Galois group of the polynomial $x^n - 1$ over any field F is cyclic.

Solution. We may assume that the characteristic does not divide n, because otherwise the Galois group is trivial. Then the roots of $x^n - 1$ form a cyclic group, and the Galois group G of $x^n - 1$ is a subgroup of automorphisms of $\mathbb{Z}_n$, in other words $G \subset \mathbb{Z}_n^*$. If $n = p$ is prime, then $\mathbb{Z}_n^*$ is cyclic as the multiplicative group of a finite field. If $n = 2p, p > 2$, then $\mathbb{Z}_{2p}^*$ is isomorphic to $\mathbb{Z}_p^*$. (The isomorphism $f : \mathbb{Z}_p^* \to \mathbb{Z}_{2p}^*$ can be given, for example, by $f(x) = x$ for odd $x, f(x) = x + p$ for even x). If $n = 4$, then $\mathbb{Z}_4^* \cong \mathbb{Z}_2$ is cyclic. A subgroup of a cyclic group is cyclic. Hence G is cyclic.

2. Show that the Galois group of $x^{15} - 1$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Solution. The Galois group of $x^{15} - 1$ is isomorphic to $\mathbb{Z}_{15}^*$. One has an isomorphism $\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. One can take 4 and 7 as generators.

3. Find the Galois groups of $x^6 - 1$ over $\mathbb{F}_5, \mathbb{F}_{25}$ and $\mathbb{F}_{125}$.

Solution. We know that the Galois group of a finite extension is always cyclic. Thus, we just have to find the degree of a splitting field. Since we have the decomposition
$$x^6 - 1 = (x-1)(x+1)\left(x^2 + x + 1\right)\left(x^2 - x + 1\right),$$

and if α is a root of x^2+x+1, then $-\alpha$ is a root of x^2-x+1, the splitting field for x^6-1 coincides with the splitting field of x^2+x+1. Note that x^2+x+1 does not have roots in $\mathbb{F}_5$, therefore it is irreducible over $\mathbb{F}_5$. Therefore the splitting field for x^2+x+1 is isomorphic to $\mathbb{F}_{25}$. Thus, the Galois group over $\mathbb{F}_5$ is isomorphic to $\mathbb{Z}_2$, the Galois group over $\mathbb{F}_{25}$ is trivial. Note that x^2+x+1 does not have roots in $\mathbb{F}_{125}$, because $\mathbb{F}_{125}$ has degree 3 over $\mathbb{F}_5$ and does not contain a subfield of degree 2. Thus, the Galois group over $\mathbb{F}_{125}$ is again $\mathbb{Z}_2$.

4. Let $F \subset E$ be an extension of finite fields. Prove that

$$|E| = |F|^{(E/F)}.$$

Solution. Let $m = (E/F)$. Choose a basis $\alpha_1, \dots, \alpha_m$ in E over F. Every element $\alpha \in E$ can be written uniquely as $\alpha = b_1\alpha_1 + \dots + b_m\alpha_m$ with $b_1, \dots, b_m \in F$. Hence $|E| = |F|^m$.

5. Let $f(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree 3. Prove that $f(x)$ is irreducible over $\mathbb{F}_{p^5}$.

Solution. Assume that $f(x)$ is reducible over $\mathbb{F}_{p^5}$. Then there is root α of $f(x)$ lying in $\mathbb{F}_{p^5}$. Then $\mathbb{Z}_p(\alpha)$ is a subfield of $\mathbb{F}_{p^5}$. On the other hand

$$(\mathbb{F}_{p^5}/\mathbb{Z}_p) = 5, (\mathbb{Z}_p(\alpha)/\mathbb{Z}_p) = 3,$$

hence 3 divides 5. Contradiction.

6. Let $q = p^k$ for some prime p, n be a number relatively prime to p, m be the minimal positive integer such that

$$q^m \equiv 1 \mod n.$$

Show that the Galois group of $x^n - 1$ over $\mathbb{F}_q$ is isomorphic to $\mathbb{Z}_m$.

Solution. Let E be the unique extension of $\mathbb{F}_q$ of degree m. We will prove that E is a splitting field of x^n-1 over $\mathbb{F}_q$. Let E^* denote the multiplicative group of E. Then E^* is cyclic of order q^m-1. Since n divides q^m-1, E^* contains a cyclic subgroup of order n. Elements of this cyclic subgroup are the roots of x^n-1. To check that E is a splitting field, we need to show that every proper subfield of E does not contain all roots for x^n-1. Indeed, let B be a subfield such that $F \subset B \subset E$. Then $|B| = q^s$ for some $s < m$. Then n does not divide $|B^*| = q^s - 1$ and therefore B^* can not contain a cyclic subgroup of order n.

To finish the problem, just note that the Galois group of x^n-1 is $\mathrm{Aut}_{\mathbb{F}_q} E \cong \mathbb{Z}_m$.