

MATH 594, WINTER 2006, PROBLEM SET 8

DUE: MONDAY, 4/9/2006

WARM-UP (NOT TO BE HANDED IN)

[DF], §14.2, exercises 17–20, 31, §14.3, 1–5.

1. EXERCISES TO BE HANDED IN

Exercise 1. Do [DF], §14.2, exercise 10.

Solution. The field is $K = \mathbb{Q}(\sqrt[8]{3}, \zeta_8) = \mathbb{Q}(\sqrt[8]{3}, i, \sqrt{2})$ is the splitting field of $x^8 - 3$ over \mathbb{Q} so K/\mathbb{Q} is Galois. The field $L = \mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q}$ is the splitting extension of $x^4 - 3$, so L/\mathbb{Q} is Galois. Since $i \notin M := \mathbb{Q}(\sqrt[4]{3})$ (because i is complex) we have $[L : \mathbb{Q}] = [L : M][M : \mathbb{Q}] = 2 \cdot 4 = 8$. $\text{Gal}(L/\mathbb{Q})$ is generated by σ, τ where $\sigma(\sqrt[4]{3}) = i^4\sqrt[4]{3}$, $\sigma(i) = i$, $\tau(\sqrt[4]{3}) = \sqrt[4]{3}$ and $\tau(i) = -i$. We have $\tau\sigma\tau^{-1} = \sigma^{-1}$ and $\text{Gal}(L/\mathbb{Q}) \cong D_8$. The only subgroup of $\text{Gal}(L/\mathbb{Q})$ of index 2 containing τ is $\langle \tau, \sigma^2 \rangle$. This shows that $\mathbb{Q}(\sqrt{2})$ is not a subfield of L , and therefore, $\sqrt{2} \notin L$. $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong Z_2$ is generated by ν defined by $\nu(\sqrt{2}) = -\sqrt{2}$. Let $N = \mathbb{Q}(\sqrt{2})L$. Then N/\mathbb{Q} is Galois. Since $\sqrt{2} \notin L$, we have $[N : \mathbb{Q}] = [N : L][L : \mathbb{Q}] = 2 \cdot 8 = 16$. In this case we have $\text{Gal}(N/\mathbb{Q}) \cong \text{Gal}(L/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = D_4 \times Z_2$. The automorphisms σ, τ of L extends to automorphisms of N such that $\sigma(\sqrt{2}) = \tau(\sqrt{2}) = \sqrt{2}$. And ν extends to an automorphism of N such that $\nu(\sqrt[4]{3}) = \sqrt[4]{3}$ and $\nu(i) = i$. So $\text{Gal}(N/\mathbb{Q})$ is generated by σ, τ, ν with relations $\tau\sigma\tau^{-1} = \sigma^{-1}$, $\sigma\nu = \nu\sigma$ and $\tau\nu = \nu\tau$. Now σ extends to an automorphism of K . We have $\sigma(\sqrt[8]{3})^2 = \sigma(\sqrt[4]{3}) = i\sqrt[4]{3}$ so $\sigma(\sqrt[8]{3}) = \zeta_8^4\sqrt[8]{3}$ or $\sigma(\sqrt[8]{3}) = \zeta_8^5 \cdot \sqrt[8]{3}$ and similarly $\sigma(\zeta_8) = \zeta_8$ or $\sigma(\zeta_8) = \zeta_8^5$. In all these cases, σ has order 8. This proves that $K \neq N$, so $[K : \mathbb{Q}] = 2 \cdot 16 = 32$. We can lift τ and ν to K as well such that $\tau(\sqrt[8]{3}) = \nu(\sqrt[8]{3}) = \sqrt[8]{3}$. One can now check that $\tau\sigma\tau^{-1} = \sigma^{-1}$ and $\tau\nu = \nu\tau$ and $\sigma\nu = \nu\sigma$. It follows that the Galois group is isomorphic to $D_{16} \times Z_2$.

Exercise 2. Do [DF], §14.2, exercise 12.

Solution. Let $\alpha = \sqrt{7 + 2\sqrt{10}}$ and $\beta = \sqrt{7 - 2\sqrt{10}}$. The roots of the polynomial are $\pm\alpha, \pm\beta$. Now $\alpha\beta = \sqrt{49 - 40} = \sqrt{9} = 3$. So the splitting field is $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$. $(\alpha + \beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2 = 20$, so $\alpha + \beta = 2\sqrt{5}$. This shows that $\sqrt{2}, \sqrt{5} \in \mathbb{Q}(\alpha)$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 4$ and $[\mathbb{Q}(\sqrt{5}, \sqrt{2}) : \mathbb{Q}] = 4$, we must

have $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5}, \sqrt{2})$. So the Galois group $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is isomorphic to $Z_2 \times Z_2$. (Note $\alpha = \sqrt{2} + \sqrt{5}$.)

Exercise 3. Do [DF], §14.2, exercise 14.

The number $\alpha = \sqrt{2 + \sqrt{2}}$ is a root of $f(x) := (x^2 - 2)^2 - 2 = x^4 - 4x^2 + 2$. Let $\beta = \sqrt{2 - \sqrt{2}}$. Then the roots of $f(x)$ are $\pm\alpha, \pm\beta$. Now $\alpha\beta = \sqrt{2} = \alpha^2 - 2$. This shows that $\beta \in \mathbb{Q}(\alpha)$, hence $\mathbb{Q}(\alpha)$ is the splitting field of $f(x)$ and $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. $f(x)$ is irreducible, because $f(x)$ has no rational roots, and it does not factor into two factors of degree 2 because $-\alpha^2$ and $\alpha\beta$ are irrational as well (these would be the possible constant terms of one of the factors). So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Some element σ in the Galois group sends α to β . So $\sigma(\sqrt{2}) = \sigma(\alpha^2 - 2) = \beta^2 - 2 = -\sqrt{2}$. And $\sigma(\beta) = \sigma(\sqrt{2}/\alpha) = -\sqrt{2}/\beta = -\alpha$. So σ acts on the roots as a 4-cycle: $\alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta \mapsto \alpha$. The Galois group is Z_4 .

Exercise 4. Do [DF], §14.2, exercise 27.

Solution.

(a) Let σ be an Automorphism with $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = -\sqrt{3}$. Then $a \cdot \sigma(a) = 2 \cdot 6 = 12$. If $a = \alpha^2$, then $(\alpha \cdot \sigma(\alpha))^2 = 12$, so $2\sqrt{3} = \sqrt{12} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})^\sigma = \mathbb{Q}(\sqrt{6})$. Contradiction because $\mathbb{Q}(\sqrt{6}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \neq \mathbb{Q}(\sqrt{6})$.

(b) Note that $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ because a is not fixed under any element of the Galois group except the identity. In particular, $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(a)$. Now $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] \leq 2$ and $\mathbb{Q}(a) \neq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ by (a). So $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$ and

$$[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] \cdot [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

The minimum polynomial $f(x)$ of $a = (2 + \sqrt{2})(3 + \sqrt{3})$ has roots $(2 \pm \sqrt{2})(3 \pm \sqrt{3})$ (just let the Galois group act on it). α is a root of $g(x) = f(x^2)$. Since $g(x)$ has degree 8, this must be the minimum polynomial. It is clear that the set of roots are $\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}$.

(c) For $\gamma = \sqrt{(2 + \sqrt{2})(3 - \sqrt{3})}$ we have $\alpha\gamma = (2 + \sqrt{2})\sqrt{6} \in F$, and for $\delta = \sqrt{(2 - \sqrt{2})(3 - \sqrt{3})}$ we have $\alpha\delta = \sqrt{12} = 2\sqrt{3} \in F$. $\mathbb{Q}(a)/\mathbb{Q}$ is Galois. The Galois group has 8 elements. Since $g(x)$ is irreducible, the Galois group acts transitively on $g(x)$.

(e) It is easy to check that $\tau \notin \langle \sigma \rangle$. So $\langle \sigma, \tau \rangle$ must be equal to the Galois group with 8 elements.

(f) The group has order 8 and it is not abelian. So it is D_8 or Q_8 . It is not D_8 because D_8 has only one cyclic subgroup of order 4.

Exercise 5. Do [DF], §14.3, exercise 7.

Solution. Assume that $p > 3$ (the polynomial has roots for $p = 2, 3$, clearly). The multiplicative group of units $\mathbb{F}_p^\times \cong Z_4$ is cyclic. Let $H \subset \mathbb{F}_p^\times$ be the subgroup of squares. Then H has index 2. If 2, 3 are not in H , then $6 = 2 \cdot 3$ lies in H . So for every p , at least one of the numbers 2, 3 or 5 is a square modulo p .

HARM DERKSEN, 3067EH, 763 2309

Office hours: **MWF 3-4pm.**

<http://www.math.lsa.umich.edu/~hderksen/math594.w06/index.html>