Honors Algebra 4, MATH 371 Winter 2010

Assignment 7

Due Friday, April 9 at 08:35

1. Let p be a prime and let K be a splitting field of $X^p-2 \in \mathbf{Q}[X]$, so $K/\mathbf{Q}$ is a Galois extension. Show that $K = \mathbf{Q}(a,\zeta)$ for $a \in K$ satisfying $a^p = 2$ and $\zeta \in K$ a primitive p th root of unity. Describe generators of $G := \mathrm{Gal}(K/\mathbf{Q})$ in terms of their actions on a and ζ, and describe G as an abstract group (in terms of generators and relations, say). Write out the diagrams of intermediate fields and groups, indicating clearly the various containments. Also indicate which subfields of K are Galois over $\mathbf{Q}$.

2. Let F be a finite field of size $\#F$, with K/F a finite extension of degree d. Prove that K/F is Galois and that $\mathrm{Gal}(K/F)$ is a cyclic group of order d with generator the automorphism of K given by
$$\alpha \mapsto \alpha^{\#F}.$$
(This automorphism is called the *arithmetic Frobenius* map of F).

3. This exercise gives Artin's proof of the fundamental theorem of Algebra. Let F be a field not of characteristic 2 and assume that all odd degree polynomials in $F[X]$ have a root in F. Let K be a quadratic extension of F with the property that every element of K has a square root in K.

   (a) Prove that any finite extension of K has degree a power of 2. (Hint: Reduce to the Galois case and then consider the fixed field of the 2-Sylow subgroup of the Galois group).

   (b) Prove that K has no non-trivial finite extensions which are Galois over F, and conclude that K is algebraically closed. (Hint: Use the fact that a non-trivial 2-group has an index 2 normal subgroup).

   (c) Let $F = \mathbf{R}$ and $K = \mathbf{R}[X]/(X^2+1)$. Explain (using the intermediate value theorem) why F satisfies the hypotheses above, and using explicit formulae, show that K also satisfies the hypotheses. Conclude that $\mathbf{C} := K$ is algebraically closed (this is the Fundamental Theorem of Algebra).

4. Determine the Galois group of the splitting field (over $\mathbf{Q}$) of $X^4 - 14X^2 + 9$, and write down the lattice of subgroups and corresponding subfields. Which subfields are Galois over $\mathbf{Q}$?

5. Fix a positive integer n and let $K := \mathbf{Q}(\zeta_n)$ for a primitive n th root of unity $\zeta_n \in \mathbf{C}$. Prove that complex conjugation $\tau \in \mathrm{Aut}(\mathbf{C})$ restricts to an automorphism of K fixing $\mathbf{Q}$, and show that the corresponding element of $\mathrm{Gal}(K/\mathbf{Q})$ corresponds to -1 under the isomorphism $\mathrm{Gal}(K/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$. Prove that the fixed field K^+ of the subgroup generated by complex conjugation is equal to the intersection $K \cap \mathbf{R}$ taken inside $\mathbf{C}$. We call K^+ the *maximal real subfield* of K.

6. This problem works out a formula for $\cos(2\pi/17)$ in terms of square-root extractions. Let $\zeta := e^{2\pi i/17}$; it is a primitive 17 th root of unity. Let $\alpha := \zeta + \zeta^{-1} = 2\cos(2\pi/17)$. Let $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ be the element determined by
$$\sigma\zeta = \zeta^3.$$

(a) Show that σ generates $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$

(b) Define the *periods* of α to be

$$\begin{aligned} \eta_1 &:= \alpha + \sigma^2\alpha + \sigma^4\alpha + \sigma^8\alpha & \eta_1' &:= \sigma\eta_1 \\ \eta_2 &:= \alpha + \sigma^4\alpha & \eta_2' &:= \sigma^2\eta_2 \\ \eta_3 &:= \sigma\eta_2 & \eta_3' &:= \sigma\eta_2' \end{aligned}$$

Prove that η_1, η_1' are the roots of $X^2 + X - 4$, that η_2, η_2' are the roots of $X^2 - \eta_1 X - 1$, that η_3, η_3' are the roots of $X^2 - \eta_1' - 1$ and that α and $\sigma^4\alpha$ are the roots of $X^2 - \eta_2 X + \eta_3$.

(c) Conclude that $\cos(2\pi/17)$ is equal to

$$\frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{2(17 - \sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}}\right)$$

7. Let F be a field and $f \in F[X]$ a monic separable polynomial of degree n. Fix a splitting field K of f and write $G := \mathrm{Gal}(K/F)$.

(a) Prove that G is a subgroup of S_n, the symmetric group on n letters. If f is irreducible, prove that G is a *transitive* subgroup of S_n with $\#G$ divisible by n. (Viewing S_n as the permutations of an n-element set T, a transitive subgroup G is one which acts transitively on these n elements, i.e. for any $x, y \in T$ there exists $g \in G$ such that $gx = y$).

(b) Prove that if n is prime and f is irreducible, then G contains an n-cycle. (Hint: use Sylow's theorem.)

(c) Suppose that f is irreducible of degree 5 and has exactly 3 real roots. Prove that G is isomorphic to S_5. (Hint: View K as a subfield of $\mathbf{C}$ and consider complex conjugation acting on K. Now use (7b) and some group theory.)

8. Keep the notation of the previous problem.

(a) Let $r_1, \ldots, r_n$ be the n distinct roots of f in K, and define the *discriminant of* f to be

$$\Delta(f) := \prod_{i,j}(r_i - r_j),$$

where the product runs over all pairs $(i, j) \in \mathbf{Z}^2$ with $1 \leq i, j \leq n$. Prove that $\Delta(f) \in F$.

(b) Prove that G is a subgroup of A_n (the alternating group) if and only if $\Delta(f)$ is a square in F. Hint: use the formula for $\Delta(f)$ above and the definition of A_n as the group of even permutations.