Dartmouth College Department of Mathematics
Math 81/111 Abstract Algebra
Winter 2024

Problem Set # 7 (Optional/Extra Credit! Upload to Canvas by midnight Tuesday, March 5)

Problems:

1. For $n \geq 0$, let $\phi_n = \zeta_{2^{n+2}}$ and $\xi_n = \phi_n + \overline{\phi}_n$. Let $K_n = \mathbb{Q}(\phi_n)$ and $K_n^+ = \mathbb{Q}(\xi_n)$.

(a) Prove that $[K_n : K_n^+] = 2$ and $[K_n^+ : \mathbb{Q}] = 2^n$. You may use the fact that $[K_n : \mathbb{Q}] = 2^{n+1}$.

(b) Determine the quadratic equation that ϕ_n satisfies over K_n^+ in terms of ξ_n.

(c) Prove that $\xi_{n+1}^2 = 2 + \xi_n$, and hence that

$$\xi_n = \sqrt{2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}}$$

where there are n nested square roots. This provides an explicit presentation for the 2-power roots of unity, showing that they are constructible (which we already knew).

(d) Prove that $K_n/\mathbb{Q}$ is Galois with group $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times$ and that $K_n^+/\mathbb{Q}$ is Galois with group cyclic of order 2^n. **Hint.** Recall the isomorphism $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times \cong C_2 \times C_{2^n}$, where C_m is a (multiplicativly written) cyclic group of order m.

2. Let p be an odd prime number, $\zeta = \zeta_p$, and $K = \mathbb{Q}(\zeta)$. We know that $K/\mathbb{Q}$ is a Galois extension with (cyclic) group $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$ and let $\sigma \in G$ be a generator. Let $H \subset G$ be the unique subgroup of index 2. Define

$$\eta_0 = \sum_{\tau \in H} \tau(\zeta), \qquad \eta_1 = \sum_{\tau \in G \setminus H} \tau(\zeta).$$

These are called the **periods** of ζ with respect to H.

(a) Prove that $\sigma(\eta_0) = \eta_1$ and $\sigma(\eta_1) = \eta_0$ and that

$$\eta_0 = \sum_{a \text{ square}} \zeta^a, \qquad \eta_1 = \sum_{a \text{ nonsquare}} \zeta^a$$

where the sums are taken over the set of squares and nonsquares, respectively, in $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) Prove that $\eta_0 + \eta_1 = -1$, and more generally, that $\sum_{\tau \in G} \tau(\zeta^a) = -1$ for any a with $p \nmid a$.

(c) Let $g = \sum_{i=0}^{p-1} \zeta^{i^2}$ be the classical **Gauss sum**. Prove that

$$g = \sum_{i=0}^{p-2} (-1)^i \sigma^i(\zeta) = \eta_0 - \eta_1.$$

(d) Prove that $\tau(g) = g$ if $\tau \in H$ and $\tau(g) = -g$ if $\tau \in G \setminus H$. Conclude, using the Galois correspondence, that $[\mathbb{Q}(g) : \mathbb{Q}] = 2$. Also conclude that $\overline{g} = g$ if -1 is a square modulo p and that $\overline{g} = -g$ if -1 is not a square modulo p, where the overline is complex conjugation. **Hint.** For the last part, recall that inversion is the same as complex conjugation for any root of unity.

(e) Prove that $g\overline{g} = p$. **Hint.** Transform $g\overline{g}$ to the double sum $\sum_{k=0}^{p-2}(-1)^k \sum_{j=0}^{p-2} \sigma^j(\sigma^k(\zeta)/\zeta)$, then use part (b).

(f) Prove that $g^2 = (-1)^{(p-1)/2} p$.

(g) Finally, conclude that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

3. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible quartic polynomial and $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x)$. Let $G \subset S_4$ be the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$.

(a) Prove that $K/\mathbb{Q}$ has no nontrivial intermediate subfields if and only if $G = A_4$ or $G = S_4$.

(b) Prove that α is constructible if and only if the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ has Galois group C_4, V_4 (Klein four), or D_8.

4. *Fundamental Theorem of Algebra.* An **ordered field** is a field F together with a subset F^+ of **positive elements** satisfying: $a, b \in F^+ \Rightarrow a + b \in F^+$ and $ab \in F^+$ and for each $a \in F$ exactly one of $a \in F^+$, $a = 0$, or $-a \in F^+$ is true.

(a) Prove that if F is an ordered field then any nonzero square is positive, that -1 is not positive, and that F has characteristic zero. Also, prove that $F(i) = F[x]/(x^2 + 1)$ is not an ordered field. **Challenge.** Prove that a field F can be ordered if and only if -1 is not a sum of squares.

(b) An ordered field F is called **real closed** if every positive element has a square root and every polynomial of odd degree over F has a root. Prove that $\mathbb{R}$ and $\mathbb{R} \cap \overline{\mathbb{Q}}$ are real closed. **Hint.** You may need a tiny bit of analysis, but try to keep it to a minimum.

(c) Prove that a real closed field does not have any nontrivial finite extensions of odd degree.

(d) Prove that if F is real closed then the only quadratic extension of F is $F(i)$, and every element of $F(i)$ has a square root.

(e) Prove that a field K is algebraically closed if and only if it does not admit any nontrivial algebraic extensions if and only if it does not admit any nontrivial finite extension.

(f) Prove that if F is a real closed field then $F(i)$ is algebraically closed. **Hint.** First, let $L'/F(i)$ be a finite extension and L/F the normal closure of L'/F. Then why is L/F a Galois extension whose group G has even order? Let $H \subset G$ be a Sylow 2-subgroup. Use the Galois correspondence with $H \subset G$ to prove that G is actually a 2-group. Remember the result from abstract algebra that every finite p-group has a subgroup of index p, and use this, with the Galois correspondence, to prove that actually G must be trivial.

(g) Deduce that $\mathbb{C}$ and $\overline{\mathbb{Q}}$ are algebraically closed.

Dartmouth College, Department of Mathematics, 6188 Kemeny Hall, Hanover, N.H. 03755
E-mail address: asher.auel@dartmouth.edu