MATH 601 (DUE 12/6)

HIDENORI SHINOHARA

Contents

1. Galois Theory VI

Exercise. (Problem 1) Let u_1, u_2, u_3, u_4 be the variables of the elementary symmetric polynomials s_1, s_2, s_3, s_4. Then $f(x) = (x - u_1)(x - u_2)(x - u_3)(x - u_4)$. Every element in $F = \mathbb{C}(s_1, \cdots, s_4)$ is a symmetric polynomial in the u_i divided by a symmetric polynomial in the u_i. $f(x)$ does not have a linear factor in $F[x]$ because the $-u_i$ in $x - u_i$ is not symmetric. Moreover, it does not have a quadratic factor in $F[x]$ because the $u_i + u_j$ in $(x - u_i)(x - u_j) = x^2 - (u_i + u_j)x + u_i u_j$ is not symmetric, so $(x - u_i)(x - u_j) \notin F[x]$. Therefore, we will use the method developed in Galois Theory IV. Let $h(y) = y^2 - \delta$ where δ is the discriminant of $f(x)$. h factors if and only if the discriminant is a perfect square. $\sigma(\prod_{i<j}(u_i - u_j)) = -\prod_{i<j}(u_i - u_j)$ under σ that corresponds to the permutation (12), so δ is not a perfect square.

Finish the $g(y)$ part. Or come up with something new.

The roots of $f(x)$ are expressible by radicals relative to F because, as shown in Problem 3 below, every transitive subgroup of S_4 is solvable.

Exercise. (Problem 2) $f(x) = x^6 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein ($p = 2$). The roots are $\{\zeta^i \sqrt[6]{2} \mid i = 0, \cdots, 5\}$ where $\zeta = e^{2\pi i/6} = (1 + \sqrt{-3})/2$. Then the splitting field L is $\mathbb{Q}(\zeta^0 \sqrt[6]{2}, \cdots, \zeta^5 \sqrt[6]{2}) = \mathbb{Q}(\zeta, \sqrt[6]{2})$. Let $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$. The minimal polynomial of $\sqrt[6]{2}$ is $x^6 - 2$, so $\sigma(\sqrt[6]{2}) = \zeta^i \sqrt[6]{2}$ for some i. The minimal polynomial of ζ is $x^2 - x + 1$, so $\sigma(\zeta) = \zeta, \overline{\zeta}$. Thus there are $6 \cdot 2 = 12$ automorphisms. This is isomorphic to D_6 because $\sqrt[6]{2} \mapsto \zeta \sqrt[6]{2}$ corresponds to rotation and $\zeta \mapsto \overline{\zeta}$ corresponds to reflection.

Exercise. (Problem 3) As discussed in the Galois Theory IV handout, the only transitive subgroups of S_4 are S_4, A_4, V_4, C_4, and groups with 8 elements. Clearly, V_4, C_4 are solvable. We showed below (Problem 2 from the Cauchy handout) that every p-group is solvable. Thus any group with 8 elements is solvable. The handout mentions $V_4 S_4$, so clearly $V_4 \trianglelefteq A_4$.

Moreover, A_4/V_4 has only 3 elements, so it is abelian. Thus $\{e\} \subset V_4 \subset A_4 \subset S_4$ is a filtration because A_4 is an index-2 subgroup of S_4. Therefore, all the transitive subgroups of S_4 are solvable, so all the roots of any quartic polynomial are expressible by radicals.

Exercise. (Problem 2) Let a prime number p be given. We will show that any group G of order p^n for some n is solvable by induction on n. When $n = 1$, $G \cong \mathbb{Z}_p$, which is abelian, so it is solvable. Suppose we have shown the proposition for some $n \in \mathbb{N}$, and let G be a group of order p^{n+1}. By Corollary 1 right above this problem statement in the handout, the center H of G is a nontrivial subgroup. Moreover, H is clearly a normal subgroup of G. Thus it makes sense to consider G/H. The order of G/H must be p^m for some $1 \leq m \leq n-1$. By the inductive hypothesis, G/H is solvable. Since every subgroup of G/H can be realized as the quotient of a subgroup of G by H[Theorem 20(1), P.99, Dummit and Foote], there must exist a sequence of subgroups $H = G_0 \leq G_1 \leq \cdots \leq G_l = G$ such that $G_0/H \trianglelefteq G_1/H \trianglelefteq \cdots \trianglelefteq G_l/H$ and $(G_{i+1}/H)/(G_i/H)$ is abelian for each i. By Theorem 19 [P.98, Dummit and Foote], $(G_{i+1}/H)/(G_i/H) \cong G_{i+1}/G_i$, so G_{i+1}/G_i is abelian for each i. $G_i/H \trianglelefteq G_{i+1}/H$ implies $G_i \trianglelefteq G_{i+1}$ for each i by Theorem 20(5) [P.99, Dummit and Foote].

We showed the existence of a sequence $H = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_l = G$ such that G_{i+1}/G_i is abelian for each i. By the inductive hypothesis, there exists a similar sequence of subgroups from $\{e\}$ to H. Therefore, G is solvable.

Exercise. (Problem 3) Let $m = 3, p = 7$. Then $|G| = 21 = pm$ with $p \nmid m$. Let t be the number of Sylow p-subgroups. By the third Sylow theorem, $t \mid m$ and $t \equiv 1 \pmod{p}$. The only number that satisfies this is 1, so every group of order 21 has a unique Sylow 7-subgroup.

Exercise. (Problem 4) Using the same idea as Problem 2 above, we will construct a filtration. Let G be an extension of H by Q. Suppose H and Q are both solvable. Since Q is solvable, there exists a filtration $\{e\} = Q_0 \trianglelefteq \cdots \trianglelefteq Q_n = Q$. Let ϕ be an isomorphism from Q to G/H. Then the $\phi(Q_i)$'s form a filtration of G/H and $\phi(Q_i) = G_i/H$ for some subgroup G_i by the same theorems that we used in Problem 2. Moreover, G_i's form a filtration from H to G. Since H is solvable, there exists a filtration from $\{e\}$ to H. By concatenating them, we obtain a filtration from $\{e\}$ to G, so G is solvable.

Exercise. (Problem 5) By Problem 3, G has a unique group H of order 7. Since conjugation preserves the order of a group, the group must be normal. Then $H \trianglelefteq G$ and $G/H \cong \mathbb{Z}_3$. Any group of prime order is abelian and thus solvable. Therefore, G is an extension of a solvable group $\mathbb{Z}_7$ by a solvable group $\mathbb{Z}_3$, so it must be solvable.

Exercise. (Problem 7) Since we are given that $\mathbb{Q}(\alpha)$ is the splitting field, every root of $f(x)$ can be expressed by multiplying, adding, dividing and subtracting rational numbers and α. This implies that $\sigma \in G = \mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is uniquely determined by $\sigma(\alpha)$. Therefore, $|G| \leq 80$.

The Galois group should be a subgroup of C_{80}, but I don't know why. Alternatively, I can show that every transitive subgroup of order ≤ 80 of S_{80} is solvable, but that sounds much harder.

Exercise. (Problem 9)

(1) By the third Sylow theorem, the number t of Sylow p-subgroups of G satisfies $t \mid q$ and $t \equiv 1 \pmod{p}$. Thus $t = 1$. Thus the subgroup H of G with p elements is normal because conjugation preserves the order of a group. G/H is a cyclic group of order q, so let $x + H$ be a generator. Then every element $g \in G$ satisfies $g + H = x^i + H$ for

a unique $i \in \{0, \cdots, q-1\}$. Then the map $G \to \mathbb{Z}_q$ such that $g \mapsto i$ is a surjective group homomorphism. A surjective homomorphism $G \to \mathbb{Z}_q$ can be constructed in a similar fashion.

(2) The problem statement simply says the existence of a homomorphism, which can be achieved by the "zero" map $g \mapsto e$. We will instead show the existence of a surjective homomorphism. In (1), we showed the existence of surjective homomorphisms $\phi_p : G \to C_p$ and $\phi_q : G \to C_q$. We have trivial homomorphisms $\psi_p : C_p \times C_q \to C_p$ and $\psi_q : C_p \times C_q \to C_q$ defined by $\psi_p(a, b) \to a$ and $\psi_q(a, b) \to b$. By the universal mapping property of the product, there must exist a unique group homomorphism $\Phi : G \to C_p \times C_q$ such that $\phi_p, \phi_q, \psi_p, \psi_q, \Phi$ all commute. Since $\phi_p = \psi_p \circ \Phi$ and $\phi_q = \psi_q \circ \Phi$ are both surjective, Φ must be surjective.

(3) Since $|G| = pq$, Φ must be bijective, so it is an isomorphism.

(4) Clearly, C_p and C_q are isomorphic to $\mathbb{Z}/p$ and $\mathbb{Z}/q$. Then the map $(a, b) \mapsto qa + b$ is an isomorphism from $\mathbb{Z}/p \times \mathbb{Z}/q$ into $\mathbb{Z}/pq$. $\mathbb{Z}/pq$ is isomorphic to C_{pq}. Therefore, G is isomorphic to C_{pq}.

Exercise. (Problem 10) By the Corollary 1 indicated in the hint, we obtain a nontrivial center C of G. By Lagrange, $|C| = p, p^2$. If $|C| = p^2$, then G is abelian, so G must be isomorphic to $\mathbb{Z}/(p^2)$ or $(\mathbb{Z}/p)^2$. Suppose $|C| = p$. Since C is normal, we will consider G/C, which is isomorphic to $\mathbb{Z}/p$. Let $x + C$ be a generator of G/C and y be a generator of C. Then every element in G can be expressed as $x^i y^j$ for some $i, j \in \mathbb{Z}/p$. However, this implies that $C = G$ because for any i, j, k, l, $(x^i y^j)(x^k y^l) = x^i x^k y^j y^l = x^k x^i y^l y^j = (x^k y^l)(x^i y^j)$ because a power of y commutes with any element. This is a contradiction, so $|C| \neq p$.