MATH 601 (DUE 12/6)

HIDENORI SHINOHARA

Contents

1. Galois Theory VI

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 $\zeta = e^{2\pi i/6} = (1 + \sqrt{-3})/2$. The 6 roots plot a hexagon on the $\mathbb{C}$-plane. $\rho(\zeta^i \sqrt[6]{2}) = \zeta^{i+1} r$ and $r(z) = \overline{z}$ are both automorphisms of the splitting field $\mathbb{Q}(\zeta, \sqrt[6]{2})$ that fix $\mathbb{Q}$. ρ and r correspond to rotation and reflection of the hexagon, so $\mathrm{Aut}(\mathbb{Q}(\zeta, \sqrt[6]{2})/\mathbb{Q})$ contains D_6.

Prove that the Galois group is exactly D_6.

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. We claim that V_4 is a normal subgroup of A_4. Every element in V_4 is a product of two disjoint cycles. Let $\sigma \in A_4$ and $p \in V_4$. Let $a = \sigma^{-1}(1), b = p(a), \sigma(b) = c$. Then $\sigma(p(\sigma^{-1}(c))) = 1$ because p is its own inverse.

What if $c = 1$?

Thus $(1c)$ is contained in $\sigma p \sigma^{-1}$. Using the same argument for the two numbers d, e in $\{d, e\} = (\{1, 2, 3, 4\} \setminus \{1, c\})$, we obtain that the cycle (de) is in $\sigma p \sigma^{-1}$. Thus $\sigma p \sigma^{-1}$ is $(1c)(de)$ where $\{1, c, d, e\} = \{1, 2, 3, 4\}$. Therefore, $\sigma p \sigma^{-1} \in V_4$. Thus $V_4 \trianglelefteq A_4$.

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.

2. Cauchy's Theorem, Finite p-groups, The Sylow theorems

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 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 $|C| \neq p$.