MATH 601 (DUE 12/6)

HIDENORI SHINOHARA

Contents

1. Jordan canonical form 1
2. Galois Theory VI 1
3. Cauchy's Theorem, Finite p-groups, The Sylow theorems 2

1. Jordan canonical form

Exercise. (Problem 3) By the theorem in the Jordan canonical form handout, there exists a basis for which the matrix M for T consists of blocks in the specified form. Let B a block of size ≥ 2 where the diagonal elements are all λ. Then the diagonal elements in B^m are all λ^m and the sub-diagonal elements in B^m are all m^{m-1}. Since $M^m = I$, $m\lambda^{m-1} = 0$. Then $\lambda = 0$. However, if $\lambda = 0$, then $\lambda^m \neq 1$. This is a contradiction, so all the blocks must be of size 1, so M is diagonal. Let $a_1, \cdots, a_m$ be the diagonal elements of M. Then M^m is a diagonal matrix with $a_1^m, \cdots, a_m^m$. Therefore, each a_i is an m-th root of unity.

2. 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 $f(x) = (x - u_1)(x - u_2)(x - u_3)(x - u_4)$. For any permutation $\sigma \in S_4$, $\phi \in \mathrm{Aut}(F(u_1, \cdots, u_n))$ determined by $\phi(u_i) = u_{\sigma_i}$ is an automorphism that fixes F because every elementary symmetric polynomial s_i is symmetric. Therefore, the Galois group is isomorphic to S_4.

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

3. 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.

Lemma 3.1. *A group of order $3 \cdot 2^k$ is solvable for any $k \geq 0$.*

Proof. When $k = 0$, this is trivial. When $k = 1$, we have a subgroup of order 3 by Cauchy, which is normal because the index is 2. Since every abelian group is solvable, Exercise 4 implies that a group of order 6 is solvable.

Suppose that we have shown this for some $k \in \mathbb{N}$. Let G be a group of order $3 \cdot 2^{k+1}$. It suffices to find a proper, nontrivial normal subgroup N of G. If such an N exists, the orders of N and G/N are either a prime power or of the form $3 \cdot 2^l$, so they are both solvable by the inductive hypothesis and Exercise 2. By the Sylow theorem, the number t of Sylow-2 group must divide 3, so $t = 1, 3$.

- If $t = 1$, then we have a normal subgroup of order 2^{k+1}, so we are done.
- Suppose $t = 3$. Let H_1, H_2, H_3 be the three Sylow-2 groups. Let $g \in G$ be given. Then $gH_1g^{-1} = H_i, gH_2g^{-1} = H_j, gH_3g^{-1} = H_k$ where $\{i, j, k\} = \{1, 2, 3\}$. Thus we can associate g to the permutation that sends 1 to i, 2 to j, and 3 to k. This association induces a group homomorphism $\Phi : G \to S_3$. By the second Sylow theorem, $\ker(\Phi) \neq G$. Since $G/\ker(\Phi)$ is a nontrivial subgroup of S_3, $G/\ker(\Phi) \leq 6$. Since $|G| \geq 3 \cdot 2^2 = 12$, $\ker(\Phi)$ is a nontrivial, proper normal subgroup of G.

Therefore, in each case, we found a nontrivial, proper normal subgroup of G. By induction, the statement is true for any $k \geq 0$. □

Exercise. (Problem 8) Lemma 3.1 shows that a group of order 192 is solvable because $192 = 3 \cdot 2^6$.

Exercise. (Problem 7) Since $\deg(f) = 80$ and f is the minimal polynomial (possibly after canceling out the first coefficient), $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 80$. Since $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ is Galois, $|\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})| = 80$. Therefore, it suffices to show that a group of order 80 is solvable. By the Sylow theorems, let t_2, t_5 be the number of subgroups of order 16 and 5. Then $t_2 \mid 5$ and $t_2 \equiv 1 \pmod 2$, so $t_2 = 1, 5$. Similarly, $t_5 \mid 16$ and $t_5 \equiv 1 \pmod 5$, so $t_5 = 1, 16$. If $t_2 = 1$ or $t_5 = 1$, then the subgroup is normal. Then the quotient group is of order 5 or 16, which, by exercise 2 above, is solvable because they are both a power of a prime. Suppose $t_2 = 5$ and $t_5 = 16$. Since the intersection of two subgroups is a subgroup, Lagrange implies that the 16 subgroups of order 5 only intersect at the identity element. Therefore, we know that at least $16 \cdot (5 - 1) = 64$ elements have order 5. Similarly, $t_2 = 5$, so there are at least $5 \cdot (16 - 1) = 75$ non-identity elements whose order divide 16. However, this is clearly impossible because 5 and 16 are coprime and we only have 80 elements. Therefore, this case is impossible.

Exercise. (Problem 8) A_5 is a simple non-abelian group, so it is not solvable. [P.3, Galois Theory VI]

$|A_5| = 5!/2 = 60$. Let $G = A_5 \times \mathbb{Z}/5\mathbb{Z}$. Then G has 300 elements and $H = \{(x, 0) \in G\}$ is a subgroup of G that is isomorphic to A_5. By lemma 1 [P.4, Galois Theory V], a solvable group cannot contain an unsolvable subgroup. Therefore, G is an unsolvable group of order 300.

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 $|C| \neq p$.

Exercise. (Problem 11) It suffices to show that every group of order 132 is solvable because it implies that every subgroup of a group of order 132 is solvable. Let $p = 11, m = 12$ and apply the third Sylow theorem. Them $t \mid 12$ and $t \equiv 1 \pmod{p}$ is satisfied only by 1 or 12.

- Suppose $t = 1$. Let H be the subgroup of order 11. Then H is normal and G/H is a group of order 12. By Sylow, the number t_4 of subgroups of order 4 of G/H is either 1 or 3 and the number t_3 of subgroups of order 3 is either 1 or 4. If $t_4 = 1$ or $t_3 = 1$, then we obtain a normal subgroup H' and $(G/H)/H'$ has 3 or 4 elements, which mean (G/H) is solvable. By Problem 4, G is solvable. Suppose $t_4 = 3$ and $t_3 = 4$. Then we have 3 distinct subgroups A_1, A_2, A_3 of order 4 and 4 distinct subgroups $B_1, \cdots, B_4$ of order 3. By Lagrange, for any $i \neq j$, $B_i \cap B_j = \{e\}$, and, for any i, j, $B_i \cap A_j = \{e\}$. However, this implies that G contains more than 12 elements. (i.e., $B_1 = \{v_1, v_2, v_3\}, B_2 = \{v_1, v_4, v_5\}, \cdots, B_4 = \{v_1, v_8, v_9\}$ and $A_1 = \{v_1, v_{10}, v_{11}, v_{12}\}$.) Therefore, this case is impossible.
- Suppose $t = 12$.

  I think this is only possible if G is abelian. But I don't know how to proceed.