

1 Homework 3.

1. Suppose p is a prime number and S_p is the symmetric group.
 - (a) Let P be a Sylow p -subgroup of S_p . Prove that $N_{S_p}(P)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$.
 - (b) Suppose G is a subgroup of S_p and G has at least two Sylow p -subgroups. Prove that G is not solvable.
 - (c) Suppose $G \subseteq S_p$ is solvable and $p \mid |G|$. Prove that the number of fixed points of every non-trivial element of G is at most 1.
 - (d) Suppose G is a subgroup of S_p which acts transitively on $[1..p]$, and for every $g \in G \setminus \{\text{id}\}$ the number of fixed points of g is at most 1. Prove that G has a normal subgroup P of order p and G/P is cyclic. In particular, G is solvable.
 - (e) Suppose G is a subgroup of S_p and $p \mid |G|$. Prove that G is solvable if and only if for every $g \in G \setminus \{\text{id}\}$, g fixes at most one point.

(**Hint.** For part (a), notice that if P_1 and P_2 are two distinct Sylow p -subgroups of S_p , then $|P_1 \cap P_2| = 1$. Argue that the union of all the Sylow p -subgroups of S_p consists of the identity and all the p -cycles. Deduce that $|N_{S_p}(P)| = p(p-1)$. Consider the affine action

$$(a, b) \in (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})^\times \curvearrowright \mathbb{Z}/p\mathbb{Z}, \quad (a, b) \cdot x := bx + a,$$

and argue why this gives an embedding of $(\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$ into $N_{S_p}(P)$ for some Sylow p -subgroup of S_p .

For part (b), first argue that if $\{X_1, \dots, X_k\}$ is a partition of $\{1, \dots, p\}$ which is invariant under G , then $k = 1$ or p . This is the case because if $k < p$, then every p -cycle has to send each X_i to itself. Then $X_1 = \{1, \dots, p\}$ and $k = 1$. Next, notice that if N is a normal subgroup of G , then the set $N \setminus \{1, \dots, p\}$ of N -orbits is invariant under G . Deduce that if N is a non-trivial normal subgroup of G , then N acts transitively on $\{1, \dots, p\}$. Now prove the claim by induction on $|G|$. If $G = [G, G]$, then G is not solvable. If not, then $N := [G, G]$ acts transitively on $\{1, \dots, p\}$. Prove that if P is a Sylow p -subgroup of G , then $P \subseteq N$; otherwise show that $p \nmid |N|$, and so N

cannot act transitively on $\{1, \dots, p\}$. By the induction hypothesis, deduce that $[G, G]$ is not solvable, and finish the proof.

For part (c), notice that by part (b), G has only one Sylow p -subgroup P , and so $G \subseteq N_{S_p}(P)$. Finish the proof using part (a).

For part (d), let G_1 be the stabilizer subgroup of 1. Then $|G| = p|G_1|$ and $G_1 \cap G_2 = \{1\}$, and so

$$G_1 \rightarrow \{2, \dots, p\}, \quad g \mapsto g(2)$$

is injective. Hence $|G_1| \leq p - 1$. Use Sylow's theorems and show $n_p = 1$. Consider the action of G_1 on the Sylow subgroup P by conjugation, and show that this gives us an embedding of G_1 into $\text{Aut}(P) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Deduce that G_1 is cyclic. Argue why $G \simeq P \rtimes G_1$ and finish the proof.

Part (e) is an immediate consequence of parts (c) and (d).)

(Remark. This result is due to Galois, and he used it in combination with his result on solvability of polynomials by radicals.)

2. Suppose p is prime, $f \in F[x]$ is irreducible, $\deg f = p$, and E is a splitting field of f over F . Suppose f has p distinct zeros in E .

- (a) Prove that there exists $\phi \in \text{Aut}_F(E)$ and $\alpha \in E$ such that

$$f(x) = (x - \alpha)(x - \phi(\alpha)) \cdots (x - \phi^{p-1}(\alpha)).$$

- (b) Prove that $\text{Gal}(E/F)$ is solvable if and only if for every two distinct zeros α and α' of f in E we have

$$E = F[\alpha, \alpha'].$$

(Hint. For part (b), use problem 1.)

3. Suppose p is prime and $f \in \mathbb{Q}[x]$ is an irreducible polynomial of degree p . Suppose f has at least two real zeros and one complex non-real zero. Let $E \subseteq \mathbb{C}$ be a splitting field of f over $\mathbb{Q}$. Prove that $\text{Gal}(E/\mathbb{Q})$ is not solvable.
4. Suppose F is a field, $f(x) \in F[x]$ is irreducible, and E is a splitting field of $f(x)$ over F . Suppose there is $\alpha \in E$ such that $f(\alpha) = f(\alpha + 1) = 0$. Prove that

- (a) Characteristic of F is a prime number p .
 - (b) Show that $\text{Aut}(E/F)$ has a subgroup of order p .
5. Suppose E is a splitting field of an irreducible separable polynomial $f \in F[x]$ over F . Suppose

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

where α_i 's are in E .

- (a) Prove that $\text{Gal}(E/F[\alpha_i])$'s are conjugate of each other as subgroups of $\text{Gal}(E/F)$.
- (b) Prove that if $\text{Gal}(E/F)$ is abelian, then $E = F[\alpha_1]$ and

$$|\text{Gal}(E/F)| = n.$$

(**Hint.** Part (a): argue that $\text{Gal}(E/F)$ acts transitively on $\{\alpha_1, \dots, \alpha_n\}$ and $G_i := \text{Gal}(E/F[\alpha_i])$ is a stabilizer subgroup of $\text{Gal}(E/F)$ with respect to α_i . For the second part, argue that in general

$$G_1 \cap \cdots \cap G_n = \{\text{id}_E\};$$

in particular, if E/F is an abelian extension, then $G_1 = 1$.)

6. Suppose F is a field of characteristic zero, $f \in F[x]$ is irreducible, and E is a splitting field of f over F . Suppose

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

for α_i 's in E . Let

$$\Delta_f := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j),$$

and $D_f := \Delta_f^2$. Let $G_{f,F}$ be subgroup of the symmetric group of $\{\alpha_1, \dots, \alpha_n\}$ which is given by the Galois group $\text{Gal}(E/F)$.

- (a) Prove that $D_f \in F$.
- (b) Prove that $\Delta_f \in F$ if and only if $G_{f,F}$ is a subgroup of the alternating subgroup.

(**Hint.** Show that for every $\sigma \in \text{Gal}(E/F)$, $\sigma(D_f) = D_f$. To show the second part, argue that $\sigma(\Delta_f) = \text{sign}(\sigma)\Delta_f$ for every $\sigma \in \text{Gal}(E/F)$.)

(**Remark.** D_f is called the discriminant of f , and it can be expressed as polynomial in terms of the coefficients of f . Find the discriminant of $x^3 - px + q$. This can be very useful to find out what the Galois group of an irreducible cubic polynomial is.)

7. Suppose F is a field, $L := F(x_1, \dots, x_n)$ is the field of fractions of $F[x_1, \dots, x_n]$. For $\sigma \in S_n$ and $f \in L$, let $T_\sigma(f) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

(a) Prove that $T : S_n \rightarrow \text{Aut}_F(L)$, $(T(\sigma))(f) := T_\sigma(f)$ is an injective group homomorphism.

(b) Let $K := \text{Fix}(T(S_n))$. Elements of K are called *symmetric functions*. Let

$$(t - x_1) \cdots (t - x_n) = t^n - s_1 t^{n-1} + s_2 t^{n-2} - \cdots + (-1)^n s_n.$$

Let $E := F(s_1, \dots, s_n)$. Prove that L is a splitting field of

$$t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n$$

over E . Deduce that $[L : E] \leq n!$.

(c) Prove that $K = E$.

(d) For $f \in L$, let $G(f) := \{\sigma \in S_n \mid T_\sigma(f) = f\}$. Prove that

$$\text{Fix}(T(G(f))) = K[f].$$

(e) Prove that $G(f) \subseteq G(g)$ for $f, g \in L$ if and only if there is $\theta \in K[t]$ such that $g = \theta(f)$.

(**Hint.** For part (c), notice that $[L : K] = |S_n|$, $E \subseteq K$, and $[L : E] \leq n!$. For part (d), observe that $\text{Gal}(L/K)$ can be identified with S_n , and using the main Galois correspondence, $\text{Gal}(L/K[f])$ gets identified with $G(f)$.)

(**Remark.** This result is known as *Lagrange's Rational Function Theorem*, and Lagrange proved this result before Galois theory was developed. Along the way, he proved some results about permutation groups, which later got generalized to what we call Lagrange's theorem in group theory!)