1 Homework 2.

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 two Sylow p-subgroups. Prove that G is not solvable.

   (c) Suppose $G \subseteq S_p$ is solvable and $p||G|$. Prove that the number of fixed points of every non-trivial element of G is at most 1.

   (d) Suppose for every $g \in G \setminus \{\mathrm{id}\}$ 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 $p||G|$. Prove that G is solvable if and only if for every $g \in G \setminus \{\mathrm{id}\}$, 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 $\{X_1, \ldots, X_k\}$ is a partition of $\{1, \ldots, p\}$ 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 $X_1 = \{1, \ldots, p\}$ and $k = 1$. Next, notice that if N is a normal subgroup of G, then the set ${}_N\backslash^{\{1,\ldots,p\}}$of N-orbits is invariant under G. Deduce that if N is a non-trivial normal subgroup of G, then N acts transitively on $\{1, \ldots, p\}$. 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 $\{1, \ldots, p\}$. 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 $\{1, \ldots, p\}$. By the induction hypothesis, deduce that $[G, G]$ is not solavable, 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

$$G_1 \to \{2, \ldots, p\}, \quad g \mapsto g(2)$$

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 $\mathrm{Aut}(P) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. 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 $\phi \in \mathrm{Aut}_F(E)$ and $\alpha \in E$ such that

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

   (b) Prove that $\mathrm{Aut}_F(E)$ is solvable if and only if for every two distinct zeros α and α' of f in E we have

   $$\mathrm{Aut}_{F[\alpha, \alpha']}(E) = \{\mathrm{id}\}.$$

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

3. Suppose $f \in \mathbb{Q}[x]$ is a monic irreducible polynomial of degree p where p is prime. Suppose $E \subseteq \mathbb{C}$ is a splitting field of f over $\mathbb{Q}$. Suppose f has exactly two non-real roots. Prove that $\mathrm{Aut}_{\mathbb{Q}}(E) \simeq S_p$.

(**Hint.** View $\mathrm{Aut}_{\mathbb{Q}}(E)$ as a subgroup G of S_p. Argue why it has an element of order p, and deduce that it has p-cycle. Show that the complex conjugation gives us a transposition in G. Use a result from group theory (Math200a, HW4, P4(b)).)

4. Suppose E/F is an algebraic extension. Let

$$E_{\text{sep}} := \{\alpha \in E \mid m_{\alpha,F} \text{ is separable in } F[x]\}.$$

   (a) Prove that E_{sep} is a subfield of E and E_{sep}/F is a separable extension.

   (b) Suppose $\text{char}(F) = p > 0$. Prove that for every $\alpha \in E$,

$$m_{\alpha,E_{\text{sep}}}(x) = x^{p^k} - \alpha^{p^k}$$

   for some non-negative integer k. In particular, $\alpha^{p^k} \in E_{\text{sep}}$ for some non-negative integer k.

   (**Hint.** Part (a); for $\alpha, \beta \in E_{\text{sep}}$, consider a splitting field L of $m_{\alpha,F}m_{\beta,F}$ over F. Argue why L/F is a separable extension, and deduce that $\alpha \pm \beta$ and $\alpha\beta^{\pm 1}$ are in E_{sep}. Hence, E_{sep} is a subfield of E, and clearly E_{sep}/E is a separable extension.

   Part (b); for every irreducible polynomial $f(x) \in F[x]$, find a non-negative integer k and a separable irreducible polynomial $f_{\text{sep}} \in F[x]$ such that $f(x) = f_{\text{sep}}(x^{p^k})$; to show this notice that if f is irreducible but not separable, then $f'(x) = 0$, and so $f(x) = f_1(x^p)$ for some irreducible polynomial $f_1(x) \in F[x]$. Use this to show that for every $\alpha \in E$, there exists an irreducible and separable polynomial $f_\alpha \in F[x]$ such that $m_{\alpha,F}(x) = f_\alpha(x^{p^k})$. Deduce that $f_\alpha = m_{\alpha^{p^k},F}$, and so $\alpha^{p^k} \in E_{\text{sep}}$; in particular $E^\times/E^\times_{\text{sep}}$ is a p-group. Suppose p^k is the order of $\alpha E^\times_{\text{sep}}$. Then $m_{\alpha,E_{\text{sep}}}(x)$ divides $x^{p^k} - \alpha^{p^k}$. Deduce that $m_{\alpha,E_{\text{sep}}}(x) = (x-\alpha)^m$ for some positive integer m. Then $\alpha^m \in E^\times_{\text{sep}}$, and so $p^k|m$. Finish the proof.)

   (**Remark.** The field E_{sep} is called the separable closure of F in E.)

5. Suppose E/F is a normal extension. Prove that E_{sep}/F is a Galois extension.

6. Suppose $F \subseteq E \subseteq K$ is a tower of fields, and K/F is an algebraic extension. Prove that K/F is separable if and only if K/E and E/F are separable.

   (**Hint.** ($\Leftarrow$) For every $\alpha \in K$, $m_{\alpha,E}(x)|m_{\alpha,F}(x)$ in $E[x]$; and so if $m_{\alpha,F}(x)$ is separable, then $m_{\alpha,E}(x)$ is separable.

   ($\Rightarrow$) Let K_{sep} be the separable closure of F in K. Then $E \subseteq K_{\text{sep}}$, and so by the converse statement, K/K_{sep} is a separable extension. On the other hand, for every $\alpha \in K$, $m_{\alpha,K_{\rm sep}}(x) = x^{p^k} - \alpha^{p^k}$ for some non-negative integer k. Deduce that $k = 0$, and so $\alpha \in K_{\rm sep}$. Therefore $K = K_{\rm sep}$.)

7. Suppose p is a prime and $E \subseteq \mathbb{C}$ is a splitting field of $x^p - 2$ over $\mathbb{Q}$. Prove that

$$\mathrm{Aut}_{\mathbb{Q}}(E) \simeq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}/p\mathbb{Z}, a \in (\mathbb{Z}/p\mathbb{Z})^\times \right\}.$$

(**Hint.** Recall why $E = \mathbb{Q}[\zeta_p, \sqrt[p]{2}]$ and $[E : \mathbb{Q}] = p(p-1)$. Deduce that $|\mathrm{Aut}_{\mathbb{Q}}(E)| = p(p-1)$ and every $\phi \in \mathrm{Aut}_{\mathbb{Q}}(E)$ is uniquely determined by the pair $(\phi(\zeta_p), \phi(\sqrt[p]{2}))$. Deduce that for every $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p\mathbb{Z}$ there exists a unique $\phi_{a,b} \in \mathrm{Aut}_{\mathbb{Q}}(E)$ such that

$$\phi_{a,b}(\zeta_p) = \zeta_p^a \quad \text{and} \quad \phi_{a,b}(\sqrt[p]{2}) = \sqrt[p]{2}\zeta_p^b;$$

moreover

$$\mathrm{Aut}_{\mathbb{Q}}(E) = \{\phi_{a,b} \mid a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z}\}.$$

Finally notice that

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto \phi_{a,b}$$

is an isomorphism.)