MAT 5210 Homework 1

1. Let G be a finite group acting on a finite set X, i.e. there is a group homomorphism $\sigma : G \to \mathrm{Aut}(X)$. We write $g \cdot x := (\sigma(g))(x)$.

   (a) Let $x \in X$. Show that the stabilizer of x,
   $$Stab_G(x) = \{g \in G : g \cdot x = x\}$$
   is a subgroup of G.

   (b) **Orbit-Stabilizer Theorem:** For any $x \in X$, let
   $$\mathrm{orb}(x) = \{g \cdot x : g \in G\} \subseteq X$$
   be the orbit of x under the action given by G. Show that
   $$|\mathrm{orb}(x)| = |G|/|Stab_G(x)|$$
   by showing that there is a bijection between the cosets of $Stab_G(x)$ and the elements of $\mathrm{orb}(x)$.

   (c) Show that if $\mathrm{orb}(x) \neq \mathrm{orb}(y)$, then $\mathrm{orb}(x) \cap \mathrm{orb}(y) = \emptyset$ and therefore that there exists a subset Y of X such that $X = \bigsqcup_{y \in Y} \mathrm{orb}(y)$.

   (d) Suppose that G acts transitively on X (i.e., for any $x \in X$, $\mathrm{orb}(x) = X$). In addition, suppose that $|X| > 1$. Show that there exists $g \in G$ such that $g \cdot x \neq x$ for any $x \in X$.

   (e) Let $g \in G$. Define a map $\psi_g : G \to G$ as follows: for any $h \in G$, $\psi_g(h) = ghg^{-1}$. Show that ψ_g is an automorphism and that $g \mapsto \psi_g$ is a homomorphism of G into $\mathrm{Aut}(G)$. Let $H = \{\psi_g \mid g \in G\}$ (one usually refers to H as the group of inner automorphisms of G). Show that H is a group and that it is normal in $\mathrm{Aut}(G)$.

   (f) Let $Z(G) = \{g \in G : ghg^{-1} = h \ \forall h \in G\}$ be the center of G. Show that $Z(G)$ is normal. In addition, show that if $G/Z(G)$ is cyclic, then G is abelian.

   (g) Using (e) and (f) (or otherwise), show that if $\mathrm{Aut}(G)$ is cyclic, then G is abelian.

2. Find the minimal polynomial for $\dfrac{\sqrt{3}}{1 + 2^{1/3}}$ over $\mathbb{Q}$; that is, the monic polynomial $m(x) \in \mathbb{Q}[x]$ of smallest possible degree satisfying
$$m\left(\frac{\sqrt{3}}{1 + 2^{1/3}}\right) = 0.$$

3. Show that if $a \in \mathbb{Z}$ is divisible by a prime p but not by p^2, then $x^n - a$ is irreducible over $\mathbb{Q}$ for all $n \geq 1$. Show also that it has no repeated roots in any extension of $\mathbb{Q}$.

4. Recall the formal derivative $D : K[x] \to K[x]$ is defined by

$$D\left(a_0 + a_1 x + \cdots + a_n x^n\right) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

   Prove that if $a, b \in K$ and $f, g \in K[x]$, then

   (a) $D(af + bg) = aDf + bDg$;

   (b) $D(fg) = fDg + gDf$;

   (c) $Dh(x) = Dg(x)Df(g(x))$ when $h(x) = f(g(x))$.

   If $a \in K$, show that

   (d) $(x - a)$ divides $f(x)$ in $K[x]$ if and only if $f(a) = 0$;

   (e) $(x - a)^2$ divides $f(x)$ in $K[x]$ if and only if $f(a) = 0 = Df(a)$.

   Deduce that if the polynomials f and Df are relatively prime in $K[x]$, then f has no multiple root.

5. (a) Show that if m is any positive integer, then the polynomial $x^{p^m} - x$ has no repeated root in any extension of fields $L : \mathbb{F}_p$.

   (b) Let
$$K = \{\alpha \in L : \alpha^{p^m} = \alpha\}$$
   be the set of roots of $x^{p^m} - x$ in the extension L. Show that K is a subfield of L.

   (c) Let n be a positive integer. Show that if m divides n, then $p^m - 1$ divides $p^n - 1$ in $\mathbb{Z}$ and $x^{p^m} - x$ divides $x^{p^n} - x$ in $\mathbb{F}_p[x]$.

6. Let $E : F$ be an extension field of prime degree ℓ, and let $\alpha \in E \setminus F$. Let M_α be the F-linear map induced by the multiplication by α:

$$\begin{aligned} M_\alpha : E &\longrightarrow E \\ u &\mapsto \alpha \cdot u \end{aligned}$$

   Show that the characteristic polynomial of M_α is equal to the minimal polynomial of α. **Hint:** Cayley-Hamilton.

7. (a) Let $f(x) = x^3 - s_1 x^2 + s_2 x - s_3 = (x-\alpha)(x-\beta)(x-\gamma) \in \mathbb{Q}[x]$ where $\alpha, \beta, \gamma \in \mathbb{C}$. Denoting $\sigma_i = \alpha^i + \beta^i + \gamma^i$ for $i \geq 0$, show that $\sigma_0 = 3$, $\sigma_1 = s_1$, and $\sigma_2 = s_1^2 - 2s_2$. Show further that

$$\sigma_r = s_1 \sigma_{r-1} - s_2 \sigma_{r-2} + s_3 \sigma_{r-3}$$

   for all $r \geq 3$.

(b) Let $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ and $\Delta = \delta^2$. Show that

$$\Delta = -4s_1^3 s_3 + s_1^2 s_2^2 + 18 s_1 s_2 s_3 - 4 s_2^3 - 27 s_3^2.$$

Hint: You may find it useful to consider the Vandermonde determinant

$$\det \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}$$

and the determinant of this matrix multiplied by its transpose to deduce first that

$$\Delta = \det \begin{pmatrix} \sigma_0 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix}.$$