B3.1 Galois Theory Sheet 1 (MT 2018)

In these problems K denotes an arbitrary field and $K[x]$ denotes the ring of polynomials in one variable x over K. If p is a prime number, then $\mathbb{F}_p$ denotes the field of integers modulo p.

1. Let E/K is a finite extension of fields and let $\alpha \in E/K$. Prove that there is a unique monic irreducible polynomial $p \in K[x]$ such that the homomorphism

$$K[x] \to K(\alpha)$$

   which maps $x \mapsto \alpha$, induces an isomorphism

$$K(\alpha) \cong K[x]/\langle p \rangle \ .$$

2. Prove the Tower Law.

3. Find the minimal polynomial for

$$\frac{\sqrt{3}}{1 + 2^{1/3}}$$

   over $\mathbb{Q}$; that is, the monic polynomial $m(x)$ of smallest possible degree with rational coefficients satisfying

$$m\left(\frac{\sqrt{3}}{1 + 2^{1/3}}\right) = 0.$$

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

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

   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. 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 $\mathbb{Q}$.

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

   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.

   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 $\mathbb{F}_p[x]$.

7. (a) Let $f(x) = x^3 - s_1x^2 + s_2x - s_3 = (x-\alpha)(x-\beta)(x-\gamma) \in \mathbb{Q}[x]$ 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
$$\Delta = -4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2.$$

   [Hint: You may find it useful to consider the Van der Monde 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
$$\Delta = \det\begin{pmatrix} \sigma_0 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix}.]$$

8. Let E/F be an extension field of prime degree ℓ and let $\alpha \in E \setminus F$. Let M_α be F-linear map induced by the multiplication by α:
$$M_\alpha : E \longrightarrow E$$
$$u \mapsto \alpha \cdot u.$$
   Show that the characteristic polynomial of M_α is equal to the minimal polynomial of α. *Hint*: Cayley-Hamilton.