HOMEWORK #4
SOLUTIONS TO SELECTED PROBLEMS

Problem 4.2. The derivation $D : K[t] \to K[t]$ is defined by $D(t^n) = nt^{n-1}$ and then extending by linearity. To prove (a), it is enough to consider the basis elements t^n of $K[t]$ over K. Indeed, one has

$$D(t^n \cdot t^m) = (n+m)t^{n+m-1} = nt^{n-1}t^m + mt^{m-1}t^n = D(t^n)t^m + t^n D(t^m)$$

For (b), note that for $f(t) = a_0 + a_1 + \cdots + a_n t^n$, one has $(Df)(t) = \sum_{i\geq 1} ia_i t^{i-1}$. Hence, $Df = 0$ implies $ia_i = 0$ for all i and since K has characteristic zero, this implies $a_i = 0$ for all i so that $f = 0$.

(c) The same reasoning gives $ia_i = 0$ for all i. Hence, if i is not divisible by p, then $a_i = 0$. We get that $f(t) = a_0 + a_p t^p + \dots$. Since K is perfect, for any $j \geq 0$ one can find b_j with $b_j^p = a_{jp}$. Taking $g(t) = b_0 + b_1 t + \dots$, we see that $g(t)^p = b_0^p + b_1^p t^p + \cdots = f(t)$, as required.

Problem 4.3. (a) One can write $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. Since ζ is a root of $x^p - 1$ but $\zeta \neq 1$, it follows that ζ is a root of the polynomial $f(x) = x^{p-1} + \cdots + x + 1$. But by Problem 3.3(b), f is irreducible in $\mathbb{Q}[x]$, hence it is the minimal polynomial of ζ over $\mathbb{Q}$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg f = p-1$.

(b) I will give a few lemmas which relate the action of field automorphisms to roots of polynomials.

Lemma 1. *Let L/K be a field extension and $\sigma \in \mathrm{Gal}(L/K)$ be an automorphism of L. If $\alpha \in L$ is a root of a polynomial $f \in K[t]$ then $\sigma(\alpha)$ is also a root of f.*

Proof. Write $f(t) = c_0 + c_1 t + \cdots + c_n t^n$ where $c_i \in K$. Since $f(\alpha) = 0$, one has

$$\begin{aligned} 0 = \sigma(f(\alpha)) &= \sigma(c_0 + c_1\alpha + \cdots + c_n\alpha^n) \\ &= \sigma(c_0) + \sigma(c_1)\sigma(\alpha) + \dots \sigma(c_n)\sigma(\alpha)^n \\ &= c_0 + c_1\sigma(\alpha) + \cdots + c_n\sigma(\alpha)^n = f(\sigma(\alpha)) \end{aligned}$$

where in the last line we used the fact the σ acts as identity on the elements of K. □

Lemma 2. *Let L/K be a field extension and suppose there exist $\alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$. If $\sigma, \tau \in \mathrm{Gal}(L/K)$ satisfy $\sigma(\alpha_i) = \tau(\alpha_i)$ for all $1 \leq i \leq n$, then $\sigma = \tau$. In other words, an automorphism of L/K is* determined *by its values on $\alpha_1, \dots, \alpha_n$.*

Proof. Let $M = \{x \in L : \sigma(x) = \tau(x)\}$. Then M is a subfield of L containing K (since both σ and τ are the identity on K) and $\alpha_1, \dots, \alpha_n$ (by assumption). So by the minimality of L we have $M = L$. □

Lemma 3. *Let L/K be a field extension and α, β be algebraic over K. Then there exists a field isomorphism $\sigma : K(\alpha) \to K(\beta)$ such that $\sigma(\alpha) = \beta$ and $\sigma_{|K} = id_K$ if and only if α and β have the same minimal polynomial over K.*

Proof. Assume that such σ exists. Then by the proof of lemma 1 we see that if $f(\alpha) = 0$ for some $f \in K[t]$ then $f(\beta) = 0$. In particular this holds when f is the minimal polynomial of α. Since f is irreducible and $f(\beta) = 0$, we get that f is also the minimal polynomial of β.

Conversely, let f be the minimal polynomial of α (and of β). Looking at the diagram

$$\begin{tikzcd} K[t]/(f) \arrow[r, equal] \arrow[d, "\varphi_\alpha"', "\simeq"] & K[t]/(f) \arrow[d, "\varphi_\beta", "\simeq"'] \\ K(\alpha) & K(\beta) \end{tikzcd}$$

where the isomorphisms $\varphi_\alpha, \varphi_\beta$ take the class $t + (f)$ to α, β respectively, we see that $\sigma := \varphi_\beta \circ \varphi_\alpha^{-1}$ is the required field isomorphism. $\square$

Having these lemmas at our disposal, we may proceed with the solution of the problem. Let $L = \mathbb{Q}(\zeta)$ and let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. By lemma 1, $\sigma(\zeta)$ must be a root of $x^p - 1$ (because ζ is), hence there exists $\alpha(\sigma)$ such that $\sigma(\zeta) = \zeta^{\alpha(\sigma)}$. Note that $\alpha(\sigma)$ cannot be zero (why?).

(c) Let $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$. Then

$$\sigma\tau(\zeta) = \sigma(\zeta^{\alpha(\tau)}) = (\sigma(\zeta))^{\alpha(\tau)} = (\zeta^{\alpha(\sigma)})^{\alpha(\tau)} = \zeta^{\alpha(\sigma)\alpha(\tau)}$$

On the other hand, $\sigma\tau(\zeta) = \zeta^{\alpha(\sigma\tau)}$.

(d) For any $0 < i < p$, the minimal polynomial of ζ^i is equal to that of ζ. Note also that $\mathbb{Q}(\zeta^i) = L$ (because p is prime hence ζ is a power of ζ^i). Therefore, by lemma 3, one can construct an automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ moving ζ to ζ^i. This shows that the mapping is onto. It is one-to-one since the value of an automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ is determined by its value on ζ by lemma 2.

Problem 4.4. (a) Suppose that $L = K[t]/(t^2 - a)$ for some $a \in K$. Let $\alpha \in L$ be a root of $t^2 - a$. Then in $L[t]$ $(t - \alpha)^2 = t^2 - \alpha^2 = t^2 - a$. Let $\sigma \in \mathrm{Gal}(L/K)$. By lemma 1, σ must map α to a root of $t^2 - a$, hence to itself, so that $\sigma(\alpha) = \alpha$). Since $L = K(\alpha)$, by lemma 2 we have $\mathrm{Gal}(L/K) = \{id_L\}$.

(b) Suppose now that $L = K[t]/(t^2 - t - a)$ for some $a \in K$. Let $\alpha \in L$ be a root of $t^2 - t - a$. Then $\alpha + 1$ is another root since $(\alpha+1)^2 - (\alpha+1) - a = \alpha^2 + 1 - \alpha - 1 - a = 0$. Since $L = K(\alpha)$, an element in $\mathrm{Gal}(L/K)$ is determined by its action on α. If $t^2 - t - a$ is irreducible (otherwise $L = K$) then by lemma 3 one can construct automorphisms of L taking α to itself or to $\alpha + 1$. So $\mathrm{Gal}(L/K)$ is a cyclic group with 2 elements.

Problem 4.5. We already know that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $[L : \mathbb{Q}] = 4$. Looking at the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3})$ and applying lemma 3 with $K = \mathbb{Q}(\sqrt{2})$ and $\alpha = \sqrt{3}$, we construct an automorphism σ_3 of L which is identity on $\mathbb{Q}(\sqrt{2})$ and takes $\sqrt{3}$ to $-\sqrt{3}$. Similarly, using the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3})(\sqrt{2})$ we construct an automorphism σ_2 of L which is identity on $\mathbb{Q}(\sqrt{3})$ and takes $\sqrt{2}$ to $-\sqrt{2}$. It is easy to see (by considering the action on the set $\{\sqrt{2}, \sqrt{3}\}$) that σ_2, σ_3 generate a four-element group isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. One always has $|\operatorname{Gal}(L/K)| \leq [L : K]$. Since $[L : K] = 4$ and we already found 4 elements in the Galois group, we deduce that $\operatorname{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Problem 4.6. The extension L/K is normal since L is a splitting field of the polynomial $t^n - a$ over K. Indeed, if α is the image of t in $L = K[t]/(t^n - a)$ and $\zeta \in K$ is a primitive n-th root of unity then $t^n - a$ splits as the product $\prod_{i=0}^{n-1}(t - \alpha\zeta^i)$.

Let $\sigma \in \operatorname{Gal}(L/K)$. By lemma 1, since α is a root of $t^n - a$, $\sigma(\alpha)$ must also be a root. Hence there exists $0 \leq i(\sigma) < n$ such that $\sigma(\alpha) = \alpha\zeta^{i(\sigma)}$.

The mapping $i : \operatorname{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z}$ is a group homomorphism; if $\sigma, \tau \in \operatorname{Gal}(L/K)$ then $\alpha\zeta^{i(\sigma\tau)} = \sigma\tau(\alpha) = \sigma(\alpha\zeta^{i(\tau)}) = \sigma(\alpha)\zeta^{i(\tau)} = \alpha\zeta^{i(\sigma)}\zeta^{i(\tau)} = \alpha\zeta^{i(\sigma)+i(\tau)}$ (note that powers of ζ are in K so the automorphisms acts trivially on them). It is one-to-one since an automorphism is determined by its action on α (lemma 2). Is it onto since by lemma 3 applied to the irreducible polynomial $t^n - a$, one can find an automorphism of L/K mapping α to any other root $\alpha\zeta^i$.

Problem 4.7. (a) The polynomial $t^5 - 2$ is irreducible in $\mathbb{Q}[t]$ by Eisenstein's criterion with the prime 2.

(b) Denote by M the splitting field of $t^5 - 2$ over $\mathbb{Q}$. Let $\zeta \in \mathbb{C}$ be a fifth root of unity. The roots of $t^5 - 2$ are $\zeta^i \sqrt[5]{2}$ for $0 \leq i < 5$. Let's prove that $M = \mathbb{Q}(\sqrt[5]{2}, \zeta)$. First $M \subseteq \mathbb{Q}(\sqrt[5]{2}, \zeta)$ because M is generated by the roots $\zeta^i \sqrt[5]{2}$ which lie in $\mathbb{Q}(\sqrt[5]{2}, \zeta)$. For the opposite inclusion, note that $\zeta = (\zeta\sqrt[5]{2})/\sqrt[5]{2}$ is a ratio of two roots of $t^5 - 2$ hence lies in M.

(c) Let $L = \mathbb{Q}(\sqrt[5]{2})$. By the irreducibility of $t^5 - 2$ we have $[L : \mathbb{Q}] = 5$. We also have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ (see Problem 4.3). Since M contains both fields, by the product formula the degree $[M : \mathbb{Q}]$ must be divisible by both 4 and 5, hence divisible by 20. On the other hand $[L(\zeta) : L] \leq 4$ because ζ is a root of $x^4 + x^3 + x^2 + x + 1$ so its minimal polynomial over L is of degree at most 4, so that $[M : \mathbb{Q}] = [L(\zeta) : L][L : \mathbb{Q}] \leq 4 \cdot 5 = 20$. We deduce that $[M : \mathbb{Q}] = 20$.

(d) The extension $L/\mathbb{Q}$ is not normal, because the polynomial $t^5 - 2$ has a root $\sqrt[5]{2}$ in L but its other roots are not in L (if there were in L we would have $M = L$ which is impossible by counting degrees).