Algebra II Assignment 3

Due Friday 18th March 2022

Please attempt all six problems in this assignment and submit your answers (before midnight on Friday 18th March 2022) by uploading your work to the Moodle page. If you have any questions, feel free to email me at adsg@hku.hk.

Problem 1. Show that every element in the subfield $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{R}$ is of the form

$$\alpha = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$$

for a unique $(a, b, c) \in \mathbb{Q}^3$. For $(a, b, c) \neq 0 \in \mathbb{Q}^3$, let

$$\frac{1}{\alpha} = a_1 + b_1\sqrt[3]{2} + c_1(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$$

with $(a_1, b_1, c_1) \in \mathbb{Q}^3$. Express (a_1, b_1, c_1) in terms of (a, b, c).

Solution. This is equivalent to say that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is a cubic extension. This follows from the irreducibility of the polynomial $f(x) = x^3 - 2$. For the second part, put ζ_3 a primitive root of $x^3 - 1$, i.e., $\zeta_3 \neq 1$. Then, you see that $1 + \zeta_3 + \zeta_3^2 = 0$. Applying this equality to the following calculation, you see

$$\begin{aligned}\frac{1}{\alpha} &= \frac{(a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2(\sqrt[3]{2})^2)(a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3(\sqrt[3]{2})^2)}{(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2)(a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2(\sqrt[3]{2})^2)(a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3(\sqrt[3]{2})^2)} \\ &= \frac{(a^2 - 2bc) + (2c^2 - ab)\sqrt[3]{2} + (b^2 - ac)(\sqrt[3]{2})^2}{a^3 + 2b^3 + 4c^3 - 6abc}.\end{aligned}$$

which completes the answer. ■

Problem 2. Let $\alpha = \sqrt{2 + \sqrt{2}} \in \mathbb{R}$.

1. Show that α is algebraic over $\mathbb{Q}$ and find the minimal polynomial of α over $\mathbb{Q}$;
2. Let $\beta = \sqrt{2 - \sqrt{2}} \in \mathbb{R}$. Show that $\beta \in \mathbb{Q}(\alpha)$ and write β as a polynomial in α with coefficients in $\mathbb{Q}$.

Solution. 1. Note that $(\alpha^2 - 2)^2 = 2$, and so α is a root of the monic polynomial $f(x) = x^4 - 4x^2 + 2$. By Eisenstein's criterion with $p = 2$, f is irreducible over $\mathbb{Q}$, and therefore f is the minimal polynomial of α over $\mathbb{Q}$.
2. $\sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$. Thus, $\beta = \sqrt{2}/\alpha = \alpha - 2/\alpha \in \mathbb{Q}(\alpha)$. It suffices to write $2/\alpha$ in terms of a polynomial in α. From the minimal polynomial of α, you see that $\alpha^4 - 4\alpha^2 = 2$. Thus, $2/\alpha = (\alpha^4 - 4\alpha^2)/\alpha = \alpha^3 - 4\alpha$. Thus, $\beta = \alpha^3 - 3\alpha$. ■

Problem 3. Suppose that $K \subset L$ is a finite field extension, and consider $\alpha \in L$ and $\alpha \notin K$.

1. Show that there exists a minimal polynomial $p(x) \in K[x]$ of α over K.
2. If β is another root of $p(x)$ in L, show that $\beta \notin K$ and $p(x)$ is also the minimal polynomial of β over K.

Solution. 1. Since $K \subset L$ is a finite extension, any $\alpha \in L \backslash K$ is algebraic over K. In other words, the prime ideal $I_\alpha = \{g \in K[x] \mid g(\alpha) = 0\} \subset K[x]$ is a non-trivial ideal. Since K is a field, $K[x]$ is a Euclidean domain, in particular a PID. Therefore, I_α has a generator which is an irreducible element in $K[x]$ with minimal degree, say $p(x)$. By rescaling if necessary, we may assume that $p(x)$ is monic. Therefore, a minimal polynomial $p(x)$ for α exists.
2. If β is another root of $p(x)$ in L, but $\beta \in K$, then $p(x)$ has a root in K, and therefore $p(x)$ admits a proper factorisation over K. This contradicts the assumption that $p(x)$ is irreducible over K. Then, $p(x)$ is an irreducible monic polynomial with root β. Suppose there exists another irreducible monic polynomial $q(x)$ with root β, of minimal degree. If $\deg(q) < \deg(p)$, then we can find $h(x), r(x) \in K[x]$ such that $p(x) = h(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(q(x))$. If r is non-zero, then $r(\beta) = 0$, which contradicts the assumption that $q(x)$ was of minimal degree. Then, $p(x) = h(x)q(x)$. Since $\deg(q) < \deg(p)$, this is a proper factorisation in $K[x]$, contradicting our assumption on $p(x)$. Therefore, $q(x)$ must have same degree as $p(x)$; the assumption that both are monic and $q(x)$ is of minimal degree implies that $p(x) = q(x)$. Therefore, $p(x)$ is the unique minimal polynomial for both α and β. ■

Problem 4. For the following $\alpha \in \mathbb{R}$, find the degree of the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$:

$$1)\ \alpha = \sqrt{1+\sqrt{3}};\quad 2)\ \alpha = \sqrt{3-\sqrt{6}};\quad 3)\ \alpha = \sqrt{3+2\sqrt{2}}.$$

Solution. 1. One has $\alpha^2 = 1 + \sqrt{3}$. Then, $(\alpha^2 - 1)^2 = 3$. Therefore, α is a root of the polynomial $f(x) = x^4 - 2x^2 - 2$. By Eisenstein's criterion with $p = 2$, this polynomial is irreducible over $\mathbb{Q}$. In other words, f is irreducible and monic with root α, so f is the minimal polynomial of α in $\mathbb{Q}[x]$. Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4$.
2. Following the approach in 1., we get $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
3. Following the approach in 1., we note that α is a root of $f(x) = x^4 - 6x^2 + 1$. Over $\mathbb{Q}$, $f(x)$ factors as $(x^2 - 2x - 1)(x^2 + 2x - 1)$; with both quadratics irreducible polynomials over $\mathbb{Q}$. Hence, one has $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. ■

Problem 5. For which values of p, q (both prime numbers) do we have $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[3]{q})$.

Solution. The element $\sqrt{p}$ is a root of the monic polynomial $x^2 - p$ which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with prime p. Therefore, $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$. Similarly, the element $\sqrt[3]{q}$ is a root of the monic polynomial $x^3 - q$ which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with prime q. Therefore, $[\mathbb{Q}(\sqrt[3]{q}) : \mathbb{Q}] = 3$. Suppose there exist primes p, q such that $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[3]{q})$. By the tower theorem, $3 = [\mathbb{Q}(\sqrt[3]{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{q}) : \mathbb{Q}(\sqrt{p})][\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt[3]{q}) : \mathbb{Q}(\sqrt{p})]$, implying 2 divides 3, a clear contradiction. Hence, no such primes p, q exist. ■

Problem 6. Let $f(x) = x^3 - 6x^2 + 4xi + (1+3i)$ in $R[x]$, where $R = \mathbb{Z}[i]$. Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ be the three roots of f.

1. Show that f is irreducible over R (Hint: you may use the fact that Eisenstein's criterion works over R any UFD, with p a prime element in R).
2. Deduce that the field extension $\mathbb{Q}(i, \alpha_1, \alpha_2, \alpha_3)$ has degree divisible by 6.

Solution. 1. The element $(1+i)$ is a prime element in $\mathbb{Z}[i]$. Notice that $(1+i)(2+i) = 1+3i$, $(1+i)2(1+i) = 4i$ and $(1+i)(-3+3i) = -6$. Furthermore, $1+i$ does not divide 1 (indeed, $N(1) = 1 < 2 = N(1+i)$), and $(1+i)^2$ does not divide $(1+3i)$ (indeed, $N(1+i)^2 = 4$ does not divide $N(1+3i) = 10$). Therefore, this polynomial is irreducible over $\mathbb{Q}[i]$ by Eistenstein's criterion with the prime $1+i$.
2. Set $L = \mathbb{Q}(i, \alpha_1, \alpha_2, \alpha_3)$. By considering the tower of extensions $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i, \alpha_1) \subset L$, we have $[L : \mathbb{Q}] = [L : \mathbb{Q}(i, \alpha_1)][\mathbb{Q}(i, \alpha_1) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$. It is easy to see that $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, and part 1. shows that $[\mathbb{Q}(i, \alpha_1) : \mathbb{Q}(i)] = 3$. Our claim follows. ■