Nepal Algebra Project 2019 Midterm exam

Tribhuvan University

July 1^{st} 2019

1. (a) *Find the minimal polynomial of $\alpha = 5 - 2\sqrt{3}$ over $\mathbb{Q}$, and* prove *that it is the minimal polynomial.*

(5 marks)

(b) *Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3})$ and that it is a normal extension of $\mathbb{Q}$.*

(5 marks)

Sol.: (a) Since $\alpha \notin \mathbb{Q}$, its minimal polynomial has degree ≥ 2. One has

$$x - \alpha = 0 \quad \Rightarrow \quad x - 5 = -2\sqrt{3} \quad \Rightarrow \quad (x-5)^2 = 12 \quad \Leftrightarrow \quad x^2 - 10x + 13 = 0.$$

The polynomial

$$f(x) = x^2 - 10x + 13$$

is *monic*, satisfies $f(\alpha) = 0$ and it is irreducible in $\mathbb{Q}[x]$. Hence it is the minimal polynomial of α.

(b) The field $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3},\ a, b \in \mathbb{Q}\}$ is another degree 2 extension of $\mathbb{Q}$ (with minimal polynomial $x^2 - 3$). From $\alpha \in \mathbb{Q}(\sqrt{3})$ one deduces the inclusion $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{3})$. Writing $\sqrt{3} = -\frac{5}{2} + \frac{1}{2}(5 - 2\sqrt{3})$ we see that $\sqrt{3} \in \mathbb{Q}(\alpha)$. Then $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\alpha)$ and therefore $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\alpha)$.

Proving that $\mathbb{Q}(\alpha)$ is a normal extension of $\mathbb{Q}$ is equivalent to verifying that the minimal polynomial f of α has all its roots in $\mathbb{Q}(\alpha)$ (see Garling, Thm. 9.1, page 78): indeed the roots of f, which are $5 \pm 2\sqrt{3}$, both lie in $\mathbb{Q}(\alpha)$.

2. *Let L/K is a finite extension of degree n and let F be an intermediate field (i.e. $K \subseteq F \subseteq L$). Prove that the degree $[F : K]$ is a divisor of n. Deduce which are the intermediate fields of an extension of degree 3.*

(10 marks)

Sol.: For the proof, see Garling, Thm.4.2, page 41.

From $K \subseteq F \subseteq L$ and $[L : F] = [L : K][K : F]$, with $[L : F] = 3$, we deduce that there are no non-trivial intermediate extensions of K.

3. *Let $f(x) = x^3 - 4x + 1 \in \mathbb{Q}[x]$.*

(a) *Prove that $f(x)$ is irreducible.*

(2 marks)

(b) *Suppose that α is a root of $x^3 - 4x + 1$ in $\mathbb{C}$. Express α^{-1} and $(1+\alpha)^{-1}$ as linear combinations, with rational coefficients, of 1, α and α^2.*

(3 marks)

(c) *Prove that α^3, α^4 and α^5 are linearly independent over $\mathbb{Q}$.*

(3 marks)

(d) *Prove that for every integer $n \neq 0$, we have $\mathbb{Q}(\alpha^n) = \mathbb{Q}(\alpha)$.*

(2 marks)

Sol.: (a) If f were reducible over $\mathbb{Q}$, then it would have at least one root in $\mathbb{Q}$, and this would be either 1 or -1. Since $f(1), f(-1) \neq 0$, we deduce that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) If is a root of $x^3 - 4x + 1$ in $\mathbb{C}$, then $\mathbb{Q}(\alpha)$ is a degree 3 extension of $\mathbb{Q}$ and there are identifications

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(x^3 - 4x + 1) \cong \{a + b\alpha + c\alpha^2,\ a, b, c \in \mathbb{Q}\}.$$

For α^{-1}, we look for $a, b, c \in \mathbb{Q}$ such that

$$(a + b\alpha + c\alpha^2)\alpha = 1 \quad \Leftrightarrow \quad a\alpha + b\alpha^2 + c\alpha^3 = 1, \quad \text{where } \alpha^3 = 4\alpha - 1,$$

$$\Leftrightarrow \quad b\alpha^2 + (4c + a)\alpha - c = 1 \quad \Leftrightarrow \quad c = -1,\ b = 0,\ a = 4.$$

Hence $\alpha^{-1} = -\alpha^2 + 4$. Check...

Similarly, for $(1 + \alpha)^{-1}$, we look for $a, b, c \in \mathbb{Q}$ such that

$$(a + b\alpha + c\alpha^2)(1 + \alpha) = 1 \quad \Leftrightarrow \quad \alpha^2(b + c) + \alpha(b + a + 4c) + (a - c) = 1.$$

We find $a = 3/4,\ b = 1/4,\ c = -1/4$ and $(1 + \alpha)^{-1} = \frac{3}{4} + \frac{1}{4}\alpha - \frac{1}{4}\alpha^2$.

(c) In $\mathbb{Q}(\alpha)$

$$a\alpha^3 + b\alpha^4 + c\alpha^5 = 0, \text{ for some } a, b, c \in \mathbb{Q}$$

if and only if (dividing by α^3)

$$a + b\alpha + c\alpha^2 = 0.$$

if and only if $a = b = c = 0$.

(d) Since $\alpha^n \in \mathbb{Q}(\alpha)$, we have

$$\mathbb{Q} \subset \mathbb{Q}(\alpha^n) \subset \mathbb{Q}(\alpha),$$

where $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ As we saw in Excercise 2, the intermediate extension $\mathbb{Q}(\alpha^n)$ either coincides with $\mathbb{Q}$ or with $\mathbb{Q}(\alpha)$.

We need to exclude that $\mathbb{Q}(\alpha^n) = \mathbb{Q}$ or, equivalently, that $\alpha^n \in \mathbb{Q}$, for $n \geq 2$.

Suppose that $\alpha^n = q \in \mathbb{Q}$, for some $n \geq 2$. Then $g(x) = x^n - q$ is a monic polynomial in $\mathbb{Q}[x]$, such that $g(\alpha) = 0$. Then f, which is the minimal polynomial of α, necessarily divides g. Now observe that all the 3 roots of f are real, while g can have at most two real roots. Contradiction.

4. *Let* $\zeta = \sqrt{3} - \sqrt{2}$.

   (a) *Show that* $\mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\zeta)$.

   (2 marks)

   (b) *Show that* $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta)$ *and that* $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\zeta)$.

   (2 marks)

   (c) *Determine the minimal polynomial of* ζ *over* $\mathbb{Q}$.

   (2 marks)

   (d) *Calculate* $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.

   (2 marks)

   (e) *Prove that* $\mathbb{Q}(\zeta)$ *is a normal extension of* $\mathbb{Q}$.

   (2 marks)

Sol.: (a) Since $\mathbb{Q}(\zeta)$ is a field containing ζ, it must also contain all it powers. As $\zeta^2 = 5 - 2\sqrt{6}$, it follows that $\sqrt{6} \in \mathbb{Q}(\zeta)$.

(b) As both $\zeta = \sqrt{3} - \sqrt{2}$ and $\zeta^3 = 9\sqrt{3} - 11\sqrt{2}$ are in $\mathbb{Q}(\zeta)$, one easily sees that also

$$\sqrt{2} = -\frac{1}{2}(\zeta^3 - 9\zeta), \quad \sqrt{3} = -\frac{1}{2}(\zeta^3 - 11\zeta)$$

are in $\mathbb{Q}(\zeta)$.

(c) One has

$$x-\alpha=0 \quad\Leftrightarrow\quad x-\sqrt{3}=-\sqrt{2} \quad\Rightarrow\quad x^2+3-2\sqrt{3}x=2 \quad\Leftrightarrow\quad x^2+1=2\sqrt{3}x \quad\Rightarrow\quad x^4+1+2x^2=12x^2.$$

The polynomial $f=x^4-10x^2+1$ is monic, satisfies $f(\zeta)=0$, and it is *irreducible* in $\mathbb{Q}[x]$. Hence it is the minimal polynomial of ζ.

(d) The degree of the extension $[\mathbb{Q}(\zeta):\mathbb{Q}]$ equals the degree of the minimal polynomial of ζ, which is 4.

To see that f is irreducible in $\mathbb{Q}[x]$, we need to check that it has no roots in $\mathbb{Q}$ and it does not factor as the product of two degree 2 monic polynomials in $\mathbb{Q}[x]$:

since ± 1 are not roots of f, then f has no rational roots. Now suppose that $f=(x^2+ax+b)(x^2+cx+d)$, for some $a,b,c,d\in\mathbb{Q}$. Then $a=c=0$, $bd=1$ and $b+\frac{1}{b}=-10$. The last equation is equivalent to $b^2+10b+1=0$, which has no rational solutions. Contradiction.

Alternatively one may reason as follows:

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\zeta),\quad \mathbb{Q}\subset\mathbb{Q}(\sqrt{3})\subset\mathbb{Q}(\zeta),\quad \mathbb{Q}\subset\mathbb{Q}(\sqrt{6})\subset\mathbb{Q}(\zeta)$$

are all quadratic intermediate extensions of $\mathbb{Q}$. If f were reducible (necessarily the product of two irreducible degree 2 monic polynomials in $\mathbb{Q}[x]$), then $\mathbb{Q}(\zeta)$ would be a quadratic extension of $\mathbb{Q}$. It would coincide with one of the above extensions. Actually it would coincide with each of them, by the results of (b) and (c). This is not the case, since for example $\sqrt{2}\notin\mathbb{Q}(\sqrt{3})$. Conclusion: f is necessarily irreducible in $\mathbb{Q}[x]$.

(e) The roots of f are $\pm(\sqrt{3}-\sqrt{2})$, $\pm(\sqrt{3}+\sqrt{2})$ and are all contained in $\mathbb{Q}(\zeta)$. (Note that $(\sqrt{3}-\sqrt{2})^2=5-2\sqrt{6}$ and $(\sqrt{3}+\sqrt{2})^2=5+2\sqrt{6}$).

Hence $\mathbb{Q}(\zeta)$ is a normal extension of $\mathbb{Q}$.

5. *Let $f=X^4-2$.*

   (a) Prove that $E=\mathbb{Q}(\sqrt[4]{2},i)$ is a splitting field for f over $\mathbb{Q}$.

   (2 marks)

   (b) Calculate $[E:\mathbb{Q}]$ and decide whether or not the extension $E/\mathbb{Q}(i)$ is normal.

   (4 marks)

   (c) Write some of the intermediate subfields for the extension $E/\mathbb{Q}$.

   (4 marks)

Sol.: (a) The roots of f are $\{\sqrt[4]{2}\zeta,\ \zeta^4=1\}=\{\sqrt[4]{2},\ -\sqrt[4]{2},\ i\sqrt[4]{2},\ -i\sqrt[4]{2}\}$. They are all contained in $E=\mathbb{Q}(\sqrt[4]{2},i)$. Thus E is a splitting field for f.

(b) The field E is a degree 8 extension of $\mathbb{Q}$: as f is the minimal polynomial of $\sqrt[4]{2}$, there is a degree 4 extension $\mathbb{Q}\subset\mathbb{Q}(\sqrt[4]{2})$. Moreover, since $\mathbb{Q}(\sqrt[4]{2})[x]$ is a subfield of $\mathbb{R}$, the f polynomial X^2+1 is irreducible over $\mathbb{Q}(\sqrt[4]{2})[x]$. Hence $[E:\mathbb{Q}]=8$.

The extension $E/\mathbb{Q}(i)$ is normal: in fact both roots $\pm i$ of the polynomial X^2+1 are contained in E.

(c) $\mathbb{Q}(\sqrt[4]{2})[x]$ and $\mathbb{Q}(i)$ are both intermediate subfields for the extension $E/\mathbb{Q}$, of degree 4 and 2, respectively.