THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 10 Solutions
25th April 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

Compulsory Part

1. (a) Note that $\alpha = 2 - \sqrt{2}$ satisfies $2 - \alpha = \sqrt{2}$ so that $(2-\alpha)^2 = 2$. Therefore $\alpha^2 - 4\alpha + 2 = 0$. In other words, α is a root of $p(x) = x^2 - 4x + 2$. By Eisenstein's criterion applied to the prime 2, $p(x)$ is irreducible over $\mathbb{Q}$. So we have $\mathbb{Q}[x]/(p) \cong \mathbb{Q}(2-\sqrt{2})$ by theorem 13.1.1.

   (b) Note that $\beta = \sqrt{1+\sqrt{3}}$ satisfies $\beta^2 = 1 + \sqrt{3}$, so that $(\beta^2 - 1)^2 = 3$. Therefore $\beta^4 - 2\beta^2 - 2 = 0$. In other words, β is a root of $q(x) = x^4 - 2x^2 - 2$. By Eisenstein's criterion applied to the prime 2, $q(x)$ is irreducible over $\mathbb{Q}$. So again by theorem 13.1.1, we have $\mathbb{Q}[x]/(q) \cong \mathbb{Q}(\sqrt{1+\sqrt{3}})$.

   (c) Note that $\gamma = \sqrt{2} + \sqrt{3}$ satisfies $\gamma^2 = 5 + 2\sqrt{2}\sqrt{3}$, so that $(\gamma^2 - 5)^2 = 24$. Therefore $\gamma^4 - 10\gamma^2 + 1 = 0$. In other words, γ is a root of $r(x) = x^4 - 10x^2 + 1$. By rational root theorem, any root of $r(x)$, if exists, must be ± 1. It is clear that those are not roots of $r(x)$. Therefore it has no linear factors. If $r(x)$ is reducible, it must be a product of two degree 2 irreducibles.

   By Gauss' theorem, we may work over $\mathbb{Z}$. Assume that $x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd$, where $b = d = 1$ or $b = d = -1$. In particular, we have $c = -a$ by looking at x^3 coefficient. Since $b + d = \pm 2$, we have $b + d + ac = \pm 2 - a^2 = -10$, i.e. $a^2 = 12$ or $a^2 = 8$. This has no solution in $\mathbb{Z}$. Therefore $r(x)$ is irreducible over $\mathbb{Z}[x]$, then by Gauss' theorem, irreducible over $\mathbb{Q}[x]$.
   By theorem 13.1.1, $\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

2. (a) Assume not, then $x^2 - 5$, being a degree 2 reducible polynomial, splits into linear factors over $\mathbb{Q}(\sqrt{2})$. Therefore there exists some element $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ so that $(a + b\sqrt{2})^2 = 5$, where $a, b \in \mathbb{Q}$. This gives $a^2 + 2b^2 + 2ab\sqrt{2} = 5$. Therefore $ab = 0$ and so $a = 0$ or $b = 0$. If $b = 0$, we have $a^2 = 5$, which is impossible in $\mathbb{Q}$. If $a = 0$, we have $2b^2 = 5$, which is also impossible in $\mathbb{Q}$. So we have come up with a contradiction. $x^2 - 5$ cannot be reducible in $\mathbb{Q}(\sqrt{2})[x]$.

   (b) By definition, we have $\mathbb{Q}(5 + \sqrt{2}) \subset \mathbb{Q}(\sqrt{2})$. (Assuming that both field extensions are contained in a bigger extension that contains both of them.) This is simply because any element in $\mathbb{Q}(5+\sqrt{2})$ is given by $f(5+\sqrt{2})/g(5+\sqrt{2})$ for some polynomials $f, g \in \mathbb{Q}$ such that $g(5+\sqrt{2}) \neq 0$. When expanded, this gives $\tilde{f}(\sqrt{2})/\tilde{g}(\sqrt{2})$, with $\tilde{g}(\sqrt{2}) = g(5+\sqrt{2}) \neq 0$, which is an element of $\mathbb{Q}(\sqrt{2})$.

In fact, the other inclusion is very similar. Given $f(\sqrt{2})/g(\sqrt{2})$, we can write for example,

$$\begin{aligned} f(\sqrt{2}) &= \sum_{k=0}^{n} a_k(\sqrt{2})^k \\ &= \sum_{k=0}^{n} a_k(5+\sqrt{2}-5)^k \\ &= \sum_{k=0}^{n} a_k \sum_{j=0}^{k} \binom{k}{j}(-5)^{k-j}(5+\sqrt{2})^j. \end{aligned}$$

The latter is a polynomial expression involving $5+\sqrt{2}$, therefore can be expressed as $\check{f}(5+\sqrt{5})$ for some $\check{f} \in \mathbb{Q}[x]$. A similar argument for g yields $f(\sqrt{2})/g(\sqrt{2}) = \check{f}(5+\sqrt{2})/\check{g}(5+\sqrt{2}) \in \mathbb{Q}(5+\sqrt{2})$.

The other equality of field extension is due to the exact same reasons.

(c) This was proven in part (a).

(d) If $2+\sqrt{5}$ and $5+\sqrt{2}$ are roots of the same irreducible polynomial $p(x) \in \mathbb{Q}[x]$. Then by theorem 13.1.1, we have $\mathbb{Q}[x]/(p) \cong \mathbb{Q}(2+\sqrt{5}) \cong \mathbb{Q}(5+\sqrt{2})$. According to part (b), this implies that $\mathbb{Q}(\sqrt{5}) \cong \mathbb{Q}(\sqrt{2})$. By part (c) (which was proven in part (a)), we know that there are no element in $\mathbb{Q}(\sqrt{2})$ whose square is 5, therefore $\mathbb{Q}(\sqrt{5})$ cannot be isomorphic to $\mathbb{Q}(\sqrt{2})$, since the image of $\sqrt{5}$ under such an isomorphism has the said property.

3. Let $a+b\gamma+c\gamma^2 = (2+\sqrt[3]{5})^{-1}$, then $(a+b\gamma+c\gamma^2)(2+\gamma) = 2a+5c+(a+2b\gamma)+(b+2c)\gamma^2 = 1$. Therefore, by comparing coefficients of both sides of the equation, we obtain $2a+5c = 1, a = -2b, b = -2c$. After solving the linear system, we get $a = \frac{4}{13}, b = \frac{-2}{13}, c = \frac{1}{13}$.

4. To find an irreducible degree 3 polynomial in $\mathbb{F}_2[x]$, it suffices to find a degree 3 polynomial that does not have a root. For example $p(x) = x^3+x+1$ does not have a root in $\mathbb{F}_2$, so it is irreducible. By theorem 13.1.1, $\mathbb{F}_2[x]/(p)$ is a field that is at the same time a vector space of dimension $\deg p = 3$ over $\mathbb{F}_2$, therefore it has $2^3 = 8$ elements.

Optional Part

1. The proof is the same as that of compulsory Q2b. Essentially, for any polynomial $p \in F[x]$, one can express $p(a+b\gamma) = \tilde{p}(\gamma)$ for some other polynomial $\tilde{p}$, and vice versa.

2. If γ is a root of irreducible polynomials p, q, then part (a) of theorem 13.1.1, we know that there are some irreducible polynomial r so that $r|p$ and $r|q$. But then p, q are themselves irreducible, so p, q, r are all the same up to a unit.

3. (a) We have $p(0) = 1, p(1) = 1, p(2) = 2$, so it has no root in $\mathbb{F}_3$ and is irreducible. So by theorem 13.1.1, $\mathbb{F}_3[x]/(p)$ is a field, namely $\mathbb{F}_3(\alpha)$ for some root of p, lying in some field extension of $\mathbb{F}_3$.

(b) Suppose $a + bx + cx^2 + (p)$ is the inverse of $x^2 + 1 + (p)$, then $(a + bx + cx^2)(1 + x^2) + (p) = 1 + (p)$. Expanding it, we obtain $a + bx + (a + c)x^2 + bx^3 + cx^4 + (p)$. But in $\mathbb{F}_3[x]/(p)$, we have $x^3 + (p) = x^2 - 1 + (p)$ and $x^4 + (p) = x(x^2 - 1) + (p) = x^2 - x - 1 + (p)$. So we have

$$(a - b - c) + (b - c)x + (a + b + 2c)x^2 + (p) = 1 + (p).$$

The linear system gives $a - b - c = 1, b = c, a + b + 2c = 0$. Solving it yields $a = \frac{3}{5}, b = c = \frac{-1}{5}$.