Fields, rings, and modules
Exercise sheet 3

https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22102/index.html

Version: March 28, 2020

Answers are due for Thursday March 26, 4PM.

Exercise 1 *Computations in an extension of* $\mathbb{Q}$ *(100 pts)*

Let $F(x) = x^3 + 2x - 2$, let $\alpha \in \mathbb{C}$ be a root of F, and let $K = \mathbb{Q}(\alpha)$.

1. (15 pts) Prove that $[K : \mathbb{Q}] = 3$.
2. (10 pts) Find $a, b, c \in \mathbb{Q}$ such that $\alpha^4 = a\alpha^2 + b\alpha + c$. Are a, b, c unique?
3. (15 pts) Find $d, e, f \in \mathbb{Q}$ such that $\frac{1}{\alpha^2+\alpha+3} = d\alpha^2 + e\alpha + f$. Are d, e, f unique?
4. (20 pts) Does $\sqrt{2} \in K$?

   Hint: Think in terms of degrees.
5. (20 pts) Find all fields L such that $\mathbb{Q} \subseteq L \subseteq K$.
6. (20 pts) Prove that $\mathbb{Q}(\alpha^2) = K$.

Solution 1

1. $F(x)$ is Eisenstein at 2 which is irreducible in $\mathbb{Z}$, so $F(x)$ is irreducible in ($\mathbb{Z}[x]$ and) $\mathbb{Q}[x]$. Since it is monic, it is the minimal polynomial of α, so

$$[K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg_{\mathbb{Q}} \alpha = \deg F = 3.$$

2. Since $0 = F(\alpha) = \alpha^3 + 2\alpha - 2$, we have $0 = \alpha F(\alpha) = \alpha^4 + 2\alpha^2 - 2\alpha$, whence

$$\alpha^4 = -2\alpha^2 + 2\alpha.$$

   We may thus take $a = -2$, $b = 2$, $c = 0$. In fact, this is the only possibility since $\alpha^2, \alpha, 1$ is a $\mathbb{Q}$-basis of K as $\deg_{\mathbb{Q}} \alpha = 3$.

3. We use the Euclidean algorithm, as when we proved that $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ in the lecture. Dividing $x^3 + 2x - 2$ by $x^2 + x + 3$ yields quotient $x - 1$ and remainder 1. Dividing by 1 will yield remainder 0 , so we stop. We have

$$F(x) = (x^2 + x + 3)(x - 1) + 1$$

so, evaluating at $x = \alpha$, we get

$$0 = (\alpha^2 + \alpha + 3)(\alpha - 1) + 1$$

whence

$$\frac{1}{\alpha^2 + \alpha + 3} = 1 - \alpha.$$

We may thus take $d = 0$, $e = -1$, $f = 1$. And gain this is the only possibility since $\alpha^2, \alpha, 1$ is a $\mathbb{Q}$-basis of K.

4. If we had $\sqrt{2} \in K$, then we would have

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset K,$$

whence

$$[K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [K : \mathbb{Q}] = 3.$$

But $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ by the same logic as in 1., since $x^2 - 2$ is Eisenstein at 2. So we would have $[K : \mathbb{Q}(\sqrt{2})] = 3/2 \notin \mathbb{N}$, absurd.

5. Given such L, we have

$$[K : L][L : \mathbb{Q}] = [K : \mathbb{Q}] = 3$$

so $[K : L] = 1$ or $[L : \mathbb{Q}] = 1$ since 3 is prime. In the first case, $L = K$, and in the second case, $L = \mathbb{Q}$. So the only such L are $L = \mathbb{Q}$ and $L = K$.

6. Let $L = \mathbb{Q}(\alpha^2)$. Then $\mathbb{Q} \subset L$, and $L \subset K$ since $\alpha^2 \in K$. By the previous question, we deduce that L is either $\mathbb{Q}$ or K. But if $L = \mathbb{Q}$, then $\alpha^2 \in L = \mathbb{Q}$, so there exists $g \in \mathbb{Q}$ such that $\alpha^2 - g = 0$. Then $G(x) = x^2 - g \in \mathbb{Q}[x]$ has α as a root, so it is divisible by the minimal polynomial of α, which is $F(x)$; that is, $F \mid G$. But this is absurd, since $\deg F = 3$ whereas $\deg G = 2$. So $L = K$.