Rings, fields, and modules
Exercise sheet 4

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU22102/index.html

Version: April 6, 2021

Email your answers to aylwarde@tcd.ie by Tuesday April 6, 4PM.

Exercise 1 *An irreducible polynomial of degree 4 (100 pts)*

Let $f(x) = x^4 + x^2 - 2x - 1 \in \mathbb{Z}[x]$.

1. (2 pts) Briefly explain why $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are fields.
2. (15 pts) Determine the factorisation of f in $(\mathbb{Z}/3\mathbb{Z})[x]$. Do not forget to prove that your factorisation is complete!

   Hint: Which of the elements of $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$ *are roots of* f *mod* 3*?*
3. (a) (5 pts) Let R be a commutative ring of characteristic 2 (recall that this means that $1+1=0$ in R). Prove that for all $a, b \in R$, $(a+b)^2 = a^2+b^2$. Deduce that more generally, for all $a_1, a_2, \cdots, a_n \in R$,

   $$(a_1 + a_2 + \cdots + a_n)^2 = a_1^2 + a_2^2 + \cdots + a_n^2.$$

   (b) (15 pts) Use the previous question to determine the factorisation of f in $(\mathbb{Z}/2\mathbb{Z})[x]$. Do not forget to prove that your factorisation is complete!
4. (3 pts) Suppose that $g(x)$ is a factor of $f(x)$ in $\mathbb{Z}[x]$. Prove that the leading coefficient of $g(x)$ is ± 1.
5. (25 pts) Prove that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

   Hint: Suppose not. In view of the previous questions, what could be the degrees of the factors of $f(x)$*?*
6. (10 pts) Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
7. (10 pts) Let $\alpha \in \mathbb{C}$ be one of the roots of $f(x)$, and let $K = \mathbb{Q}(\alpha)$. Prove that $[K : \mathbb{Q}] = 4$, and give a $\mathbb{Q}$-basis of K.
8. (15 pts) Express $\frac{1}{\alpha - 1}$ as a polynomial in α with rational coefficients.

Solution 1

1. We know that for $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ is a field iff. n is prime; this is indeed the case for $n = 2$ and $n = 3$.

2. We begin by looking for roots of $f(x)$ mod 3. We have $f(0) = -1 \neq 0 \in \mathbb{Z}/3\mathbb{Z}$ so 0 is not a root, $f(1) = -1$ so 1 is not a root either, and $f(2) = 15 = 0 \in \mathbb{Z}/3\mathbb{Z}$, so $2 = -1$ is the only root of $f(x)$ in $\mathbb{Z}/3\mathbb{Z}$. Therefore, $f(x)$ is divisible by $x+1$ in $(\mathbb{Z}/3\mathbb{Z})[x]$; in order to find the cofactor, we Euclidean-divide $f(x)$ by $x+1$ in $(\mathbb{Z}/3\mathbb{Z})[x]$, which means that we reduce all the coefficients mod 3. We find remainder 0 (as expected), and quotient $g_3(x) = x^3 - x^2 - x - 1 \in (\mathbb{Z}/3\mathbb{Z})[x]$. If g_3 had a root in $\mathbb{Z}/3\mathbb{Z}$, then this root would also be a root of $f(x)$, so it can only be -1; yet $g_3(-1) = -2 \neq 0 \in \mathbb{Z}/3\mathbb{Z}$, so g_3 has no root. As $\deg g_3 = 3$ and as $\mathbb{Z}/3\mathbb{Z}$ is a field, this proves that $g_3(x)$ is irreducible. In conclusion, the complete factorisation of f in$(\mathbb{Z}/3\mathbb{Z})[x]$ is

$$f(x) = (x+1)(x^3 - x^2 - x - 1).$$

3. (a) As $2 = 0 \in R$, we have $(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$. We deduce that

$$(a_1 + a_2 + \cdots + a_n)^2 = a_1^2 + a_2^2 + \cdots + a_n^2$$

for all n by induction on n.

(b) We observe that mod 2, $f(x) = x^4 + x^2 + 1 = (x^2)^2 + x^2 + 1^2$. As $(\mathbb{Z}/2\mathbb{Z})[x]$ has characteristic 2, we conclude from the previous question that $f(x) = (x^2 + x + 1)^2$. This factorisation is complete iff. $x^2 + x + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ is irreducible; but if it were not, then as its degree is 2 and as $\mathbb{Z}/2\mathbb{Z}$ is a field, it would have a root, yet neither of the elements 0 and 1 of $\mathbb{Z}/2\mathbb{Z}$ are roots. In conclusion, the complete factorisation of f in$(\mathbb{Z}/2\mathbb{Z})[x]$ is

$$f(x) = (x^2 + x + 1)^2.$$

4. Since $g(x)$ is a factor of $f(x)$ in $\mathbb{Z}[x]$, we have $f(x) = g(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Let $a_n x^n$ (resp. $b_m x^m$) be the leading term of $g(x)$ (resp. of $h(x)$). Then the leading term of $g(x)h(x)$ is abx^{n+m}. However, this is also the leading term x^4 of $f(x)$, so $ab = 1$ and $m + n = 4$; in particular $a = b = \pm 1$ as $a, b \in \mathbb{Z}$.

5. Suppose that $g(x)$ is a factor of $f(x)$ in $\mathbb{Z}[x]$ of degree n. Then $g(x)$ is still a factor of $f(x)$ in $\mathbb{Z}/2\mathbb{Z}$, and its degree in $(\mathbb{Z}/2\mathbb{Z})[x]$ is still n as its leading coefficient is $\pm 1 \neq 0 \in \mathbb{Z}/2\mathbb{Z}$. In view of question 3b, we thus have $n \in \{0, 2, 4\}$ by uniqueness of factorisation in the UFD $(\mathbb{Z}/2\mathbb{Z})[x]$. Similarly, $g(x)$ is also a factor over $\mathbb{Z}/3\mathbb{Z}$, whence $n \in \{0, 1, 3, 4\}$. Therefore, $n = 0$ or $n = 4$.

If $n = 0$, then $g(x) \in \mathbb{Z}$ is constant; as $f(x)$ is primitive, $g(x) = \pm 1 \in \mathbb{Z}[x]^\times$ is a unit.

If $n = 4$, then the cofactor $h(x) = f(x)/g(x)$ of $g(x)$ has degree 0, so again it is a unit oin $\mathbb{Z}[x]$.

Therefore, any non-trivial facotrisation of $f(x)$ in $\mathbb{Z}[x]$ involves a unit, so $f(x)$ is irreducible in $\mathbb{Z}[x]$.

6. Since $f(x)$ is irreducible in $\mathbb{Z}[x]$, Gauss theorem informs us that either it is an irreducible constant in $\mathbb{Z}$ or it remains irreducible in $\mathbb{Q}[x]$. Since it is not the former, it is the latter.

7. Since $f(x)$ is monic and irreducible over $\mathbb{Q}$, it is the minimal polynomial of α over $\mathbb{Q}$. Therefore, $[K : \mathbb{Q}] = \deg f = 4$, and $(1, \alpha, \alpha^2, \alpha^3)$ is a $\mathbb{Q}$-basis of K.

8. Let $g(x) = x - 1$, which is coprime to $f(x)$ in $\mathbb{Q}[x]$ since they are both irreducible and clearly not associates (not the same degree). As $\mathbb{Q}[x]$ is a PID, Bézout ensures the existence of $c(x), d(x) \in \mathbb{Q}[x]$ such that $f(x)c(x) + g(x)d(x) = 1$, which yields $\frac{1}{\alpha-1} = d(\alpha)$ at $x = \alpha$. In order to find $d(x)$, we use the Euclidean algorithm. Dividing $f(x)$ by $g(x)$ yields remainder $r(x) = f(1) = -1$ and quotient $q(x) = x^3 + x^2 - 2x$, so $f(x) = g(x)q(x) + r(x)$; we may therefore take $d(x) = q(x)$, whence

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

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they is not worth any points, and you do not have to submit them. However, you can try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercises.

Exercise 2 *Some irreducible polynomials*

1. Prove that $x^5 + 6x + 12$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

2. Let $f = x^7y + y^5 - xy^3 + 2x \in \mathbb{C}[x, y]$. Express f as an element of $\mathbb{C}[y][x]$, and then as an element of $\mathbb{C}[x][y]$. Prove that f is irreducible in $\mathbb{C}[x, y]$.

Solution 2

1. This follows from the fact that this polynomial is Eisenstein at the prime number $p = 3$ (but NOT at $p = 2$, since $2^2 \mid 12$!)

2. Under the natural identification $\mathbb{C}[x, y] = \mathbb{C}[y][x]$ (resp. $\mathbb{C}[x][y]$), we have $f = yx^7 + (2 - y^3)x + y^5$ (resp. $f = y^5 - xy^3 + x^7y + 2x$). In particular, we observe that f is Eisenstein at x (this makes sense because $\mathbb{C}[x]$ is a UFD in which x is irreducible, and in which $x^2 \nmid 2x$); it is therefore irreducible in $\mathbb{C}[x][y] = \mathbb{C}[x, y]$ (and even in $\mathbb{C}(x)[y]$).

Exercise 3 *Computations in an extension of* $\mathbb{Q}$

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

1. Prove that $[K : \mathbb{Q}] = 3$.
2. Find $a, b, c \in \mathbb{Q}$ such that $\alpha^4 = a\alpha^2 + b\alpha + c$. Are a, b, c unique?
3. 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. Does $\sqrt{2} \in K$?

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

Solution 3

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 $L = K$.