Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Faculty of Engineering, Mathematics and Science

School of Mathematics

JS/SS Maths/TP/TJH **Semester 2, 2019**

MAU22102 Rings, fields, and modules — Review exam

Dr. Nicolas Mascot

Instructions to Candidates:

This is a review exam, meant to help you prepare for the actual exam.

Question 1 *Irreducibility*

1. Let K be a field. Determine the units of the polynomial ring $K[x]$. Explain.

2. Let R be a commutative ring. Define what it means for an element of R to be *irreducible*. Spell out the definition in the case $R = K[x]$, where K is a field as above.

3. Let again K be a field. For which non-negative integers $n \geqslant 0$ is the polynomial x^n irreducible in $K[x]$?

4. Give an example of an element of $\mathbb{Q}[x]$ which has degree 2020 and is irreducible.

Solution 1

1. Since K is a field, it is a domain, so we have $\deg(fg) = deg(f) + \deg(g)$ for all $f, g \in K[x]$. Therefore, if $f \in K[x]^\times$, then $\deg f = 0$. Thus $K[x]^\times = K^\times = K \setminus \{0\}$ since K is a field.

2. An element $x \in R$ is irreducible if x is non zero, not a unit, and if whenever $x = yz$ for some $y, z \in R$, then $y \in R^\times$ or[1] $z \in R^\times$.

   Thus an element $f(x)$ of $K[x]$ is irreducible if it is non-constant (this takes care simultaneously of non-zero and non-unit) and if the only factorisations $f(x) = g(x)h(x)$ with $g, h \in K[x]$ ar those where g or h is constant (so they look like $f = \frac{1}{2} \cdot (2f)$.

3. For $n = 0$ we have $x^n = 1$ which is a unit and therefore not irreducible in $K[x]$.

   For $n = 1$, we have that $x^n = x$ is irreducible, since it is non-constant but cannot be factored as a product of two non-constant polynomials (because the degree is additive).

   Finally, for $n \geqslant 2$ we can write $x^n = xx^{n-1}$, so x^n is not irreducible since neither factor is constant.

   So the only n such that x^n is irreducible is $n = 1$.

4. Let $p \in \mathbb{N}$ be a prime number (e.g. $p = 29$), and consider $f(x) = x^{2020} + p$. It is Eisenstein at p since it is monic, p divides all the non-leading coefficients, and p^2 does

[1] not both, for else we would have $x = yz \in R^\times$.

not divide the constant coefficient. By Eisenstein's criterion, it is irreducible in $\mathbb{Q}[x]$ (and also in $\mathbb{Z}[x]$).

Question 2 *Radicals and extensions*

Let $\alpha = \sqrt{2}i \in \mathbb{C}$, so that $\alpha^2 = -2$, and let $K = \mathbb{Q}(\alpha)$.

1. Prove that α is algebraic over $\mathbb{Q}$, and determine its minimal polynomial.
2. Determine $[K : \mathbb{Q}]$, and find a $\mathbb{Q}$-basis of K.
3. Let $\beta = \sqrt{2}$. Using the previous question, prove that $\beta \notin K$.
4. Is it possible to prove that $\beta \notin K$ by degree considerations only?
5. Determine the minimal polynomial of α over K. Comment
6. Prove that β is algebraic over K, and determine its minimal polynomial over K. Also
7. Let $L = K(\beta)$. Determine $[L : \mathbb{Q}]$, and find a $\mathbb{Q}$-basis of L.
8. Prove that $i \in L$. What are its coordinates on the $\mathbb{Q}$-basis of L that you fond at the previous question?
9. Is it true that $L = \mathbb{C}$?

Solution 2

1. α is a root of the non-zero polynomial $f(x) = x^2 + 2 \in \mathbb{Q}[x]$, so it is algebraic over $\mathbb{Q}$. Besides $f(x)$ is irreducible in $\mathbb{Q}[x]$ because it is Eisenstein at $p = 2$ (other possibility: since it has degree 2, if it factored over $\mathbb{Q}$ then it would hve a linear factor, hence a root in $\mathbb{Q}$; but its roots are $\pm\alpha$ and neither is in $\mathbb{Q}$) and it is monic, so it is the minimal polynomial of α over $\mathbb{Q}$.

2. $d = [K : \mathbb{Q}]$ is the degree of the minimal polynomial of α, hence 2 by the previous question. We also deduce that
$$(1, \alpha, \alpha^2, \cdots, \alpha^{d-1}) = (1, \alpha)$$
is a $\mathbb{Q}$-basis of K.

3. By the previous question, each element of K is uniquely of the form $x+y\alpha$ for $x, y \in \mathbb{Q}$. So if $\sqrt{2} \in K$, we would have $a, b \in \mathbb{Q}$ such that $\sqrt{2} = a + b\alpha$. Squaring yields $2 = a^2 + 2ab\alpha - 2b^2$, i.e.
$$2 + 0\alpha = (a^2 - 2b^2) + 2ab\alpha \in K.$$
Since each element of K is **uniquely** of the form $x + y\alpha$ for $x, y \in \mathbb{Q}$, we can deduce that $a^2 - 2b^2 = 2$ and that $2ab = 0$. In particular, one of a or b is 0. This is absurd: if $a = 0$, then $2 = a^2 - 2b^2 = -2b^2$ so $b^2 = -1$ in contradiction with $b \in \mathbb{Q}$, and if $b = 0$, then $2 = a^2 - 2b^2 = a^2$ in contradiction with $\in \mathbb{Q}$. Thus $\sqrt{2} \notin K$.

4. We prove as in the first question that β is algebraic of degree 2 over $\mathbb{Q}$. So if we had $\beta \in K$, we would have $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq K$ whence $[K : \mathbb{Q}] = [K : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$ i.e. $2 = 2[K : \mathbb{Q}(\beta)]$. This is not a contradiction, it just says that $[K : \mathbb{Q}(\beta)] = 1$, which means that the inclusion $\mathbb{Q}(\beta) \subseteq K$ would actually be an equality. SO this approach does not seem to lead anywhere.

5. The minimal polynomial of α over K is *NO LONGER* $f(x) = x^2+2$, but $x-\alpha \in K[x]$. The reason is that $f(x)$ becomes reducible in $K[x]$, since it factors a $(x - \alpha)(x + \alpha)$; in contrast, $x - \alpha$ is monic, and it is irreducible over K because it has degree 1, and degrees are additive.

   In fact, this argument shows that $x - \alpha$ remains irreducible over any extension of K, so it is the minimal polynomial of α over any extension of K. It is not however the minimal polynomial of α over $\mathbb{Q}$, since it does not lie in $\mathbb{Q}[x]$ because of its constant term. In summary, over an extension E of $\mathbb{Q}$, the minimal polynomial of α is $x - \alpha$ if $\alpha \in E$, and $x^2 + 2$ if $\alpha \notin E$ (because if it were not $x^2 + 2$, then $x^2 + 2$ would be reducible E and hence have a root in E, contradiction since its roots are $\pm\alpha$).

6. β is a root of $g(x) = x^2 - 2 \in K[x]$ so it is algebraic over K (and even over $\mathbb{Q}$, since $g(x)$ actually lies in $\mathbb{Q}[x]$). $g(x)$ is monic, and Eisenstein at $p = 2$ so it is irreducible over $\mathbb{Q}$, but this does **NOT** guarantee that $x^2 - 2$ remains irreducible over K (compare with the previous question); all we can deduce from this is that $x^2 - 2$ is the minimal polynomial of β over $\mathbb{Q}$, but this is not the question!

   Suppose $g(x)$ were reducible over K. Then by additivity of the degree, it would have a linear factor over K, so it would have a root in K. But its roots are $\pm\beta$, and we have shown that they do not lie in K, contradiction. So $g(x)$ remains irreducible over K, and is thus the minimal polynomial of β over K.

7. By the tower law we have $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}]$. We already know that $[K : \mathbb{Q}] = 2$, and $[L : K] = [K(\beta) : K]$ is the degree of the minimal polynomial over β over K, which is 2 by the previous question. So $[L : \mathbb{Q}] = 4$. Besides, we know that $(1, \alpha)$ is a $\mathbb{Q}$-basis of K, and by a similar argument that $(1, \beta)$ is a K-basis of L; by the tower law, we conclude that $(1, \alpha, \beta, \alpha\beta)$ is a $\mathbb{Q}$-basis of L.

   Note: See how this question and the previous would collapse if instead of $\beta \notin K$ we had $\beta \in K$.

8. Simply note that $i = \alpha/\beta \in L$ since $\alpha, \beta \in L$ and L is a field. Besides, $\alpha\beta = 2i$, so the coordinates of i on the $\mathbb{Q}$-basis $(1, \alpha, \beta, \alpha\beta)$ of L are $(0, 0, 0, 1/2)$ (which do lie in $\mathbb{Q}$).

9. Absolutely not! For instance, $\mathbb{C}$ contains numbers that are transcendental over $\mathbb{Q}$, such as π or e, and therefore $[\mathbb{C} : \mathbb{Q}] = \infty$ (another way to say this is that L, being a finite extension of $\mathbb{Q}$, is an algebraic extension of $\mathbb{Q}$, so it only contains numbers that are algebraic over $\mathbb{Q}$, and hence not π nor e).

   Note: $i \in L$ does not imply that $L = \mathbb{C}$; in fact, the smallest extension of $\mathbb{Q}$ containing i is $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, which is a strict subfield of L. On the other hand, since by definition $\mathbb{C} = \mathbb{R}(i)$, any extension of $\mathbb{R}$ (not $\mathbb{Q}$) containing i must be at least as large as $\mathbb{C}$.

Question 3 *Annihilators and torsion elements*

Let R be a commutative domain, and let M be an R-module. Given an element $m \in M$, we define its *annihilator* as the subset

$$\mathrm{Ann}(m) = \{r \in R \mid rm = 0\}$$

of R.

1. An example: determine $\mathrm{Ann}(m)$ if $m = 0$.

2. Prove that for any $m \in M$, $\mathrm{Ann}(m)$ is an ideal of R.

3. We say that an element $m \in M$ is *torsion* if its annihilator is not reduced to $\{0\}$, i.e. if there exists $r \in R$, $r \neq 0$ such that $rm = 0$, and we define

   $$M_{\mathrm{tor}} = \{m \in M \mid m \text{ is torsion}\}.$$

   Prove that M_{tor} is a submodule of M.

4. We say that M is *torsion-free* if $M_{\mathrm{tor}} = \{0\}$. Prove that if M is free of finite rank, then M is torsion-free.

5. Prove that for any module M, the quotient module M/M_{tor} is torsion-free.

Solution 3

1. If $m = 0$, then $rm = r0 = 0$ for all $r \in R$, so $\mathrm{Ann}(m) = R$.

2.
   - First of all, $0 \in \mathrm{Ann}(m)$ since $0m = 0$.
   - If $a, a' \in \mathrm{Ann}(m)$, i.e. $am = a'm = 0$, then $(a + a')m = am = a'm = 0$, so $a + a' \in \mathrm{Ann}(m)$.
   - If $a \in \mathrm{Ann}(m)$ and $r \in R$, then $(ra)m = r(am) = r0 = 0$, so $ra \in \mathrm{Ann}(m)$.

   Thus $\mathrm{Ann}(m)$ is an ideal of R.

   Remember: To solve this kind of question, proceed in to times: first, determine what you must prove (i.e remember the definition of an ideal), and then, prove it.

3. - Let $m, m' \in M_{\rm tor}$. By definition, this means we have nonzero elements $r, r' \in R$ such that $rm = 0 = r'm'$. Then $rr'(m+m') = rr'm+rr'm' = r'(rm)+r(r'm) = r'0 + r0 = 0$, and $rr' \neq 0$ since $r, r' \neq 0$ and R is a domain; this shows that $m + m' \in M_{\rm tor}$, so $M_{\rm tor}$ is stable by sum.
   - Let now $m \in M_{\rm tor}$ and $s \in R$. By definition, we have a nonzero $r \in M$ such that $rm = 0$. Then $r(sm) = (rs)m = (sr)m = s(rm) = s0 = 0$, so $sm \in M_{\rm tor}$. This shows that $M_{\rm tor}$ is stable by multiplication by R.

   Thus $M_{\rm tor}$ is a submodule of M.

   Remember: Same advice as for the previous question!

4. Since M is free of finite rank, it admits a finite R-basis $(m_1, m_2, \cdots)$. Let $m \in M_{\rm tor}$. Then in particular $m \in M$, so we can express it (uniquely) as

$$m = r_1 m_1 + r_2 m_2 + \cdots$$

   for some $r_1, r_2, \cdots \in R$. Since $m \in M_{\rm tor}$, there exists a nonzero $r \in R$ such that $rm = 0$. Spelling this out, we get

$$0 = rm = (rr_1)m_1 + (rr_2)m_2 + \cdots .$$

   Since the m_i form a basis, they are linearly independent, so we must have $0 = rr_1 = rr_2 = \cdots$ (shorter: invoke the uniqueness of the decomposition of $0m_1 + 0m_2 + \cdots = 0 = (rr_1)m_1 + (rr_2)m_2 + \cdots$). Since R is a domain, $rr_1 = 0$ implies $r = 0$ or $r_1 = 0$, but $r \neq 0$ by assumption so $r_1 = 0$. Similarly $r_2 = 0$, etc. Thus

$$m = r_1 m_1 + r_2 m_2 + \cdots = 0m_1 + 0m_2 + \cdots = 0.$$

   This proves that $M - {\rm tor}$ is reduced to $\{0\}$, as wanted.

   Remember: Same advice as for the previous questions!

5. Let $\bar{m} \in (M/M_{\rm tor})_{\rm tor}$, we have to prove that $\bar{m} = \bar{0}$. Since $\bar{m}$ is torsion, there exists a nonzero $r \in R$ such that $r\bar{m} = \bar{0}$. Let $m \in M$ be an element projecting to $\bar{m} \in M/M_{\rm tor}$, then rm projects to $r\bar{m} = \bar{0}$, so $rm \in M_{\rm tor}$ by the definition of the quotient. So there

exists a nonzero $s \in R$ such that $s(rm) = 0$. But then $(sr)m = s(rm) = 0$, and $sr \neq 0$ since $r, s \neq 0$ by assumption and R is a domain, so m is torsion, i.e. $m \in M_{\text{tor}}$. By ths means that $\bar{m} = \bar{0}$, again by definition of the quotient. So we are done.