Solutions to Exam Algebraic Structures,
June 21st, 2019, 9.00pm–12.00pm, MartiniPlaza, L. Springerlaan 2.
Please provide complete arguments for each of your answers. The exam consists of 3 questions each subdivided into 4 parts. You can score up to 3 points for each part, and you obtain 4 points for free.
In this way you will score in total between 4 and 40 points.

(1) In this exercise we denote the ring $\mathbb{Z}[t]/(t^3)$ by R. Elements of R we write as $f(t) \bmod (t^3)$, for some $f(t) \in \mathbb{Z}[t]$.

(a) Show that $t+1 \bmod (t^3)$ is a unit in R and find its inverse.

- *Answer:* $1+t^3 = (1+t)(1-t+t^2) \in \mathbb{Z}[t]$. *So in* R, *we have* $1 = (1+t)(1-t+t^2) \bmod (t^3)$.

(b) Does, apart from $1 \bmod (t^3)$ and $0 \bmod (t^3)$, the ring R contain any idempotent (i.e., an element $\gamma \in R$ with $\gamma^2 = \gamma$)?

- *Answer: Let* $\gamma = a + bt + ct^2 \bmod (t^3) \in R$ *such that* $\gamma^2 = \gamma$. *So we have* $\gamma^2 = a^2 + 2abt + (b^2+2ac)t^2 \bmod (t^3) = a + bt + ct^2 \bmod (t^3)$. *This implies* $a = a^2$ *and since* $a \in \mathbb{Z}$, *we have* $a = 0$ *or* 1. *If* $a = 0$, *then* $b = c = 0$. *If* $a = 1$, *then* $b = c = 0$. *So the only idempotent elements in* R *are* $0 \bmod (t^3)$ *and* $1 \bmod (t^3)$.

(c) Show that no unitary rings R_1 and R_2 exist in which $0 \neq 1$, such that $R \cong R_1 \times R_2$.

- *Answer: The only unitary subrings of* R *are* R *and the ring of constants. Hence* R *cannot be isomorphic to the product of non-trivial unitary rings.*
- *Answer 2: By part (b), we find that* R *contains no idempotents other than* 0 *and* 1, *whereas* $R_1 \times R_2$ *contains more of these (such as* $(0,1)$*). Since isomorphisms preserve idempotents, we conclude that they cannot be isomorphic.*

(d) For $a, b, c \in \mathbb{Z}$, show that $a + bt + ct^2 \bmod (t^3)$ is a unit in R, if and only if $a = \pm 1$.

- *Answer:* $u = a + bt + ct^2 \bmod (t^3)$ *is a unit in* R *iff there exists* $(a' + b't + c't^2 \bmod (t^3))$ *such that*

$$\begin{aligned} 1 \bmod (t^3) &= (a + bt + ct^2 \bmod (t^3))(a' + b't + c't^2 \bmod (t^3)) \\ &= aa' + (ab' + ba')t + (ac' + ca' + bb')t^2 \bmod (t^3). \end{aligned}$$

So if u is a unit then $aa' = 1$, hence $a = \pm 1$. On the other hand, $\pm 1 - bt + (\pm b^2 - c)t^2 \bmod (t^3)$ is the inverse of $\pm 1 + bt + ct^2 \bmod (t^3)$. Hence if $a = \pm$ then u is a unit.

(2) Consider the ring $R = \mathbb{Q}[x, y]$.

(a) Show that if $P \subset R$ is a prime ideal, then $P \cap \mathbb{Q}[x]$ is a principal ideal in $\mathbb{Q}[x]$ that is either generated by 0 or by an irreducible element of $\mathbb{Q}[x]$.

- *Answer: The ring* $\mathbb{Q}[x]$ *is a subring of* $\mathbb{Q}[x, y]$. *Suppose that* $a, b \in \mathbb{Q}[x]$ *are such that* ab *is an element of* $P \cap \mathbb{Q}[x]$. *Then*

$ab \in P$ hence a or b is in P (as P is a prime ideal). This implies that $a \in P \cap \mathbb{Q}[x]$ or $b \in P \cap \mathbb{Q}[x]$. This concludes that $P \cap \mathbb{Q}[x]$ is a prime ideal in $\mathbb{Q}[x]$. Moreover, since $P\mathbb{Q}[x]$ is a PID, the statement follows.

(b) Show that $\mathbb{Q}[x, y] \cdot (x - y^2)$ is a prime ideal in R.
- *Answer: Define evaluation homomorphism $\mathrm{ev}_{y^2} : \mathbb{Q}[x, y] \to \mathbb{Q}[y] : f(x, y) \mapsto f(y^2, y)$. Then the kernel $\ker(\mathrm{ev}_{y^2})$ is the ideal $\mathbb{Q}[x, y] \cdot (x - y^2)$. So we have $\mathbb{Q}[x, y]/(x - y^2) \cong \mathrm{ev}_{y^2}(\mathbb{Q}[x, y]) \subset \mathbb{Q}[y]$. Since $\mathbb{Q}[y]$ is an integral domain, this ideal is prime.*
- *Answer 2: Let $R' = \mathbb{Q}[x]$, where $R = R'[y]$. Then $y^2 - x$ is an Eisenstein polynomial at x, so it is irreducible. Since $\mathbb{Q}[x, y]$ is a UFD (by applying Theorem V.4.1 twice), we have that $(y^2 - x)$ is a prime ideal by Theorem V.3.2.*

(c) Show that $x^3 + y^3 + 1 \in R$ is irreducible.
- *Answer: Let $R' = \mathbb{Q}[y]$. Then $R = R'[x]$. Then we can write $x^3 + (y^3 + 1) \in R'[x]$. This is an Eisenstein polynomial for the irreducible element $y + 1 \in R'$.*

(d) Prove that the ideal in R generated by the two polynomials $x - y^2$ and $x^3 + y^3 + 1$ is a maximal ideal in R.
- *Answer: The evaluation map ev_{y^2} in (b) is surjective hence gives an isomorphism $\mathbb{Q}[x, y]/(x - y^2) \cong \mathbb{Q}[y]$. Theorem II.3.10 tells us that $\mathbb{Q}[x, y]/(x - y^2, x^3 + y^3 + 1) \cong \mathbb{Q}[y]/(y^6 + y^3 + 1)$. Since $y^6 + y^3 + 1$ is irreducible in $\mathbb{Q}[y]$ and $\mathbb{Q}[y]$ is a PID, we have that $\mathbb{Q}[y]/(y^6 + y^3 + 1)$ is a field and hence $(x - y^2, x^3 + y^3 + 1)$ is a maximal ideal in $\mathbb{Q}[x, y]$.*

(3) In this final exercise, R denotes the field $\mathbb{F}_2[t]/(t^4 + t + 1)$.

(a) Show that indeed R is a field.
- *Answer: Since $\mathbb{F}_2[t]$ is a PID, it suffices to show that $f(t) := t^4 + t + 1$ is an irreducible element in $\mathbb{F}_2[t]$. This polynomial does not have a linear factor over $\mathbb{F}_2$ since $f(0) \neq 0 \neq f(1)$ modulo 2. Suppose that $f = gh$ for some monic irreducible polynomials of degree 2 in $\mathbb{F}_2[t]$. Since the only degree 2 irreducible polynomial in $\mathbb{F}_2[t]$ is $t^2 + t + 1$, we obtain $(t^2 + t + 1)^2 = t^4 + t + 1$. But this does not hold. Hence $t^4 + t + 1$ is irreducible.*

(b) Find the minimal polynomial of $t^2 + t \bmod (t^4 + t + 1)$ over the prime field of R.
- *Answer: Let $\alpha := t + (t^4 + t + 1) \in R$. We have $R \cong \mathbb{F}_2(\alpha)$, where α is a root of the polynomial $t^4 + t + 1 \in \mathbb{F}_2[t]$. The prime field of R is $\mathbb{F}_2$. So we want to find the minimal polynomial of $\alpha^2 + \alpha$ over $\mathbb{F}_2$. The minimal polynomial of $\alpha^2 + \alpha$ is of degree at least 2 as $\alpha^2 + \alpha \notin \mathbb{F}_2$. Moreover, we see that $(\alpha^2 + \alpha)^2 + \alpha^2 + \alpha + 1 = 0$. So the minimal polynomial of $\alpha^2 + \alpha$ is $t^2 + t + 1 \in \mathbb{F}_2[t]$.*

(c) Show that $\varphi : f(t) \bmod (t^4 + t + 1) \mapsto f(t + 1) \bmod (t^4 + t + 1)$ is a well-defined automorphism of the field R.

- *Answer:* Well-definedness: *Let $g(t)$ and $h(t)$ be two polynomials in $\mathbb{F}_2[t]$ which are in the same class* mod (t^4+t+1), *i.e.,* $g(t) = h(t) + s(t)\cdot(t^4+t+1)$, *for some polynomial $s(t)$. Then we have*

$$\begin{aligned} g(t+1) &= h(t+1) + s(t+1)\cdot((t+1)^4 + (t+1) + 1) \\ &= h(t+1) + s(t+1)\cdot(t^4+t+1) \end{aligned}$$

  So $g(t+1)$ and $h(t+1)$ are in the same equivalence class. Hence the map is well-defined and in particular $\varphi(\overline{0}) = \overline{0}$.
  Field homomorphism:
  1. $\varphi(\overline{1}) = \overline{1}$ is clear.
  2. $\varphi(\overline{f(t)} + \overline{g(t)}) = \varphi(\overline{(f+g)(t)}) = \overline{(f+g)(t+1)} = \overline{f(t+1)} + \overline{g(t+1)} = \varphi(\overline{f(t)}) + \varphi(\overline{g(t)})$.
  3. Similary, $\varphi(\overline{f(t)}\cdot\overline{g(t)}) = \varphi(\overline{f(t)})\cdot\varphi(\overline{g(t)})$. *To put it simply, once we have shown that φ is well-defined, given $f(t)$ and $g(t)$, it is clear that the equivalence classes of $(f+g)(t+1)$ and $f(t+1)+g(t+1)$ are the same (and likewise for the product).*
  Automorphism: *Since R is a finite field it is enough to show that φ is injective. Since non-trivial field homomorphisms are injective, this holds.*

(d) What are the possible orders of elements in the group of units $R^\times$?

- *Answer: III.5.4 Corollary tells us that the group of units in a field is cyclic. The order of the group is $16-1=15$. Hence the possible orders of elements in this group are $1, 3, 5,$ and 15.*