THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2024-25
Tutorial 8
7th November 2024

- Tutorial exercise would be uploaded to blackboard on Mondays provided that there is a tutorial class on that Thursday. You are not required to hand in the solution, but you are advised to try the problems before tutorial classes.
- Please send an email to echlam@math.cuhk.edu.hk if you have any questions.

Most rings that we will encounter or use are rings with unity, so unless specified otherwise, "a ring" will mean "a ring with unity".

1. Let R be a commutative ring, show that for any $a \in R$, the evaluation map $\mathrm{ev}_a : R[x] \to R$ defined by $\mathrm{ev}_a(f(x)) = f(a)$ is a ring homomorphism. Determine its kernel.
2. If R is not commutative, we can still define the polynomial ring $R[x]$ as before. Give an example showcasing that the evaluation map is no longer a ring homomorphism.
3. For a commutative ring R, prove that it is a field if and only if it contains precisely two ideals.
4. Determine whether or not S is a subring of R in the following cases:
   (a) S is the set of rational numbers of the form $\frac{a}{b}$ where b is not divisible by 3. $R = \mathbb{Q}$.
   (b) S is the set of linear combinations of $\{1, \cos(nt), \sin(nt)\}$ for $n \in \mathbb{Z}$, $R = C(\mathbb{R})$ the set of continuous functions on $\mathbb{R}$.
5. Determine the set of units in $\mathbb{Z}_n$. (Hint: What are the generators of $\mathbb{Z}_n$ as groups?)
6. Let I, J be ideals of a ring R, define $I + J = \{a + b : a \in I, b \in J\}$, show that $I + J, I \cap J$ are again ideals of R.
7. Let R, R' be rings, prove that $R \times R'$ with addition given by $(a, a') + (b, b') = (a + a', b + b')$ and multiplication given by $(a, a')(b, b') = (ab, a'b')$ endow $R \times R'$ with the structure of a ring with additive identity given by $(0, 0)$ and multiplicative identity given by $(1, 1)$.
8. Show that $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$.
9. Is $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ as rings?
10. Are $\mathbb{Z}[x]/\langle x^2 + 7\rangle$ and $\mathbb{Z}[x]/\langle 2x^2 + 7\rangle$ isomorphic?
11. Determine the ring structure of $\mathbb{Z}[x]/\langle 6, 2x - 1\rangle$ and $\mathbb{Z}[x]\langle x^2 + 3, 5\rangle$ in terms of more familiar rings.
12. Show that a finite field F has order a power of a prime: $|F| = p^k$.
13. Suppose that $a^2 = a$ for every $a \in R$, does R necessarily have characteristic 2?

14. Let R be a commutative ring and $a \in R$, consider the quotient $R' = R[x]/\langle ax-1\rangle$.

    (a) Show that any element $\beta \in R'$ can be written as $[bx^k]$ for some $b \in R$, here $[bx^k]$ is the class of bx^k, i.e. $[bx^k] = bx^k + \langle ax-1\rangle$ in the quotient.

    (b) Show that the ring homomorphism $\varphi : R \to R'$ by $\varphi(b) = [b]$ has kernel given by those b with $a^n b = 0$ for some n.

    (c) Show that R' is the zero ring if and only if $a^n = 0$ for large enough n.

15. Determine whether the following polynomials are irreducible in their respective polynomial rings.

    (a) $f(x) = x^3 + 2x^2 + x - 9 \in \mathbb{Q}[x]$.

    (b) $f(x) = 2x^7 - 15x^6 + 60x^5 - 18x^4 + 9x^3 - 12x^2 + 6x + 24 \in \mathbb{Q}[x]$.

    (c) $f(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + ... + x^2 + x + 1 \in \mathbb{Z}_p[x]$.

    (d) $f(x) = x^4 - x - 1 \in \mathbb{Q}[x]$

    (e) $f(x,y) = x^2 + y^2 \in \mathbb{C}[x,y]$

    (f) $f(x,y) = y - x^2 \in \mathbb{Q}[x,y]$.

16. (a) Show that $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$.

    (b) Prove that $x^4 + 1$ is reducible in $\mathbb{Z}_p[x]$ for every prime p by looking at the following three cases:

    i. If $-1 = a^2$ for some $a \in \mathbb{Z}_p$.

    ii. If $2 = b^2$ for some $b \in \mathbb{Z}_p$.

    iii. Otherwise, since the group of unit $\mathbb{Z}_p^\times$ is a cyclic group of even order, both $-1, 2$ have odd order, so their product has even order, i.e. $-2 = c^2$ for some $c \in \mathbb{Z}_p$.