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

- The tutorial solutions are written for reference and proofs will be sketched briefly. You should try to fill in the details as an exercise. Please send an email to echlam@math.cuhk.edu.hk if you have any further questions.

1. It is clear that $\mathrm{ev}_a(f+g) = (f+g)(a) = f(a)+g(a) = \mathrm{ev}_a(f)+\mathrm{ev}_a(g)$ and $\mathrm{ev}_a(fg) = (fg)(a) = f(a)g(a) = \mathrm{ev}_a(f)\mathrm{ev}_a(g)$. The kernel is given those $f \in R[x]$ where $f(a) = 0$. By factor theorem, in $\mathrm{ev}_a(f) = f(a) = 0$, then $f(x)$ is divisible by $x - a$, the converse is clearly true, so $\ker(\mathrm{ev}_a) = \langle x - a\rangle$.

2. If R is not commutative, then the polynomial ring is very pathological, for example, recall the quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. We can turn it into a ring by allowing the elements $\{1, i, j, k\}$ to be added formally with no relations, i.e. we define the quaternion numbers to be $Q = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{R}\}$ with addition the obvious way, multiplication inherited from Q_8, additive identity $0+0i+0j+0k$ and multiplicative identity $1+0i+0j+0k$. In the polynomial ring $Q[x]$, $(x-i)(x+i) = x^2+1 = (x+i)(x-i)$, however $(j-i)(j+i) = j^2 - ij + ji - i^2 = -2ij \neq 2ij = j^2 + ij - ji - i^2 (j+i)(j-i)$. So the evaluation map is not a homomorphism.

3. Suppose R is a field, then every nonzero element is invertible, if I is a nonzero ideal, then $a \in I \implies r = ra^{-1} \cdot a \in I$ for any $ra^{-1} \in I$, therefore $I = R$. So there are only two ideals. Conversely, if I only has two ideals, they are necessarily the whole ring and the zero ideal, therefore for any $0 \neq a \in R$, $\langle a\rangle = R$ and so $1 \in I \implies 1 = ba = ab$ for some $b \in R$.

4. (a) Suppose $\frac{a}{b}, \frac{c}{d}$ are rational so that b, d are not divisible by 3, then in $\frac{ac}{bd}, \frac{ad+bc}{bd}$, it is clear that bd is also not divisble by 3. Also $1 = \frac{1}{1}$ with 1 is not divisble by 3, so it is a subring (with unit).

   (b) By secondary school M2, we know $\cos(mt)\cos(nt) = \frac{1}{2}[\cos(m+n)t + \cos(m-n)t]$, $\sin(mt)\cos(mt) = \frac{1}{2}[\sin(m+n)t + \sin(m-n)t]$, and $\sin(mt)\sin(nt) = \frac{1}{2}[-\cos(m+n)t + \cos(m-n)t]$. So sums and products of $a_0 + \sum_{m=1}^{M}\cos(mt) + \sum_{n=1}^{N}\sin(nt)$ can be written as linear combinations of those functions again. And it contains $0, 1$, so it must be a subring.

5. The units in $\mathbb{Z}_n$ are given by those k that has an inverse $\mod n$. Suppose that there is $j \in \{1, ..., n\}$ so that $j \cdot k \equiv 1$, then $\underbrace{k + k + ... + k}_{\text{j times}} \equiv 1 \mod n$ implies that k is a generator of the additive group of $\mathbb{Z}_n$. From group theory, we know that this only occurs when $\gcd(k, n) = 1$. So there should be $\varphi(n)$ many units in $\mathbb{Z}_n$, where φ is the Euler totient function.

   The group structure is more difficult to identify. One can start by proving that the group of units in $\mathbb{Z}_{p^k}$ is cyclic for p prime, then apply Chinese remainder theorem to obtain that the group of units in $\mathbb{Z}_n$ in general is a product of those of $\mathbb{Z}_{p^k}$'s, hence is also cyclic.

6. Let I, J be ideals, then for $a_1+b_1 \in I+J$ and $a_2+b_2 \in I+J$ clearly $(a_1+b_1)+(a_2+b_2) \in I+J$ and $r(a_1+b_1) = ra_1 + rb_1 \in I+J$ since I, J are ideals, likewise for additive inverse. Now if $a, b \in I \cap J, r \in R$, similarly $a+b, ra, -a \in I \cap J$.

7. We have $R \times R'$ with addition forms an abelian group because it's just the product group. Associativity and distributivity of product follows from that of each ring.

8. Define a homomorphism $\mathbb{R}[x] \to \mathbb{C}$ by $f(x) \mapsto f(i)$. It is a homomorphism because it is the composition $\mathbb{R}[x] \hookrightarrow \mathbb{C}[x] \xrightarrow{\mathrm{ev}_i} \mathbb{C}$. Surjectivity follows from the observation $a + bx \mapsto a + bi$. The kernel of this map is given by those $f(x)$ with $f(i) = 0$. We know the minimal polynomial of i is given by x^2+1 and $\mathbb{R}[x]$ is a PID, therefore kernel is $\langle x^2+1\rangle$. By first isomorphism theorem $\mathbb{C} \cong \mathbb{R}[x]/\langle x^2+1\rangle$.

9. (Essentially just the Chinese remainder theorem) We can define a homomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ by just taking $a \mapsto (a \mod 2, a \mod 3)$. Since both rings have the same cardinality, we just need to check injectivity: if $a \equiv 0 \mod 2$ and $a \equiv 0 \mod 3$, then a is divisible by both 2 and 3, hence divisible by 6, so $a = 0 \in \mathbb{Z}_6$.

10. They are not isomorphic. This follows from the observation that if we have an isomorphism $\mathbb{Z}[x]/\langle 2x^2+7\rangle \to \mathbb{Z}[x]/\langle x^2+7\rangle$, it must send $\mathbb{Z} \to \mathbb{Z}$ by considering image of 1. In the former ring, -7 is divisible by 2 since $2 \cdot x^2 \equiv -7$. It follows that in the latter ring, -7 is also divisible by 2. Suppose $2f(x) + \langle x^2+7\rangle = -7 + \langle x^2+7\rangle$, then $x^2+7 \mid 2f(x)+7$. Let's say $2f(x)+7 = (x^2+7)\sum_{k=0}^n a_k x^k$, then

$$\begin{aligned}
2f(x) &= \sum_{k=0}^n a_k x^{k+2} + \sum_{k=0}^n 7a_k x^k - 7 \\
&= 7(a_0 - 1) + 7a_1 x + \sum_{k=2}^n (a_{k-2} + 7a_k)x^k + a_{n-1}x^{n+1} + a_n x^{n+2}.
\end{aligned}$$

   Since 2 divides all the coefficients of the RHS, we deduce that a_0 is odd, a_1 is even, and inductively a_k is even (resp. odd) implies that a_{k+2} is also even (resp. odd). However, a_{n-1} and a_n have to be both even, this gives a contradiction. So -7 cannot be divisible by 2, so there cannot be an isomorphism between the rings.

   Remark: There is a simpler proof using "integral elements". Alternatively, one can also try to show that $2(x^2+4) = 2x^2+8 \equiv 1 + \langle 2x^2+7\rangle$ implies that 2 is invertible, and similar derive a contradiction from showing that 2 cannot be invertible in the other ring.

11. One can first quotient out the integer to obtain $\mathbb{Z}_6[x]/\langle 2x-1\rangle$, let's represent the class of $f(x)$ by $[f(x)]$. We only need to determine the ring structure for the classes $[n]$ where $n = 0, ..., 5$ and also $[x^k]$, since every other class $[f(x)]$ can be reduced to one of those. we have $[0] = [3 \cdot (2x-1)] = [6x-3] = [3]$, therefore $[1] = [4]$ and $[2] = [5]$. Now notice that $[2x] = 1$, so we have $[x] = [4x] = [2 \cdot 2x] = [2]$. Therefore, we only have 3 nontrivial classes: $[0], [1], [2]$ and it's clear the ring is isomorphic to $\mathbb{Z}_3$ at this point.

    For $\mathbb{Z}_5[x]/\langle x^2+3\rangle$, all classes can be reduced to $[ax+b]$. Notice that $1 = [x^2+4] = [x^2-1] = [x+1][x+4]$, $1 = [x+2][x+3]$ and similarly $[3x][x] = [3x^2] = [3][2] = [1]$. In general, any nonzero $a \in \mathbb{Z}_5$ has an inverse (it is a unity since it is coprime to 5), and for $a \neq 0$, the class $[ax+b] = [a][x+ba^{-1}]$ is invertibe since both $[a]$ and $[x+k]$ are invertible in the ring. Hence, $\mathbb{Z}_5[x]/\langle x^2+3\rangle$ is (the) field of 25 elements.

Remark: That's all we are going to talk about finite fields. There are a lot more to talk about them and you will see them again in Math3040.

12. Let's say p is the characteristic of F, then p is a prime otherwise F has zero divisors. Now suppose that another prime q also divides order of F, then applying Cauchy's theorem on the abelian group $(F, +)$ gives a nontrivial element x so that $q \cdot x = 0$. But $p \cdot x = 0$ following from characteristic. Since the primes are coprime, $ap + bq = 1$ for some $a, b \in \mathbb{Z}$, therefore $x = (ap+bq)\cdot x = ap \cdot x + bq \cdot x = 0$, which is a contradiction. Therefore fields must have order p^n where $p = \mathrm{char}(F)$.

13. Note that $a = a^2 = (-a)^2 = -a$, so R has characteristic 2.

14. (a) For any $\beta \in R'$, we can write $\beta = [f(x)] = [\sum_{k=0}^n b_k x^k]$ for some polynomial $f(x) \in R[x]$. Then $\beta = [b_0 + ... + b_n x^n] = [(ab_0 + b_1)x + ... + b_n x^n] = ... = [bx^n]$ where $b = \sum_{k=0}^n b_k a^{n-k}$.

    (b) Suppose that $\varphi(b) = [b] = 0$, then $b \in \langle ax-1\rangle$, let $p(x) = \sum_{k=0}^n c_k x^k \in R[x]$ so that $(ax-1)\sum_{k=0}^n c_k x^k = b$ in the polynomial ring. Therefore

$$b = \sum_{k=0}^{n} ac_k x^{k+1} - \sum_{k=0}^{n} c_k x^k = ac_n x^{n+1} + \sum_{k=1}^{n}(ac_{k-1} - c_k)x^k - c_0.$$

    Matching the coefficients, we have

$$\begin{aligned} b &= -c_0 \\ c_1 &= ac_0 \\ &\vdots \\ c_n &= ac_{n-1} \\ ac_n &= 0 \end{aligned}$$

    Hence $a^n b = 0$. Conversely, if $a^n b = 0$ for some n, then $[b] = [b(ax)^n] = [ba^n x^n] = 0$. So $b \in \ker \varphi$.

    (c) Clearly if $a^n = 0$ for large enough n, then by part (a), since every element $\beta \in R'$ can be expressed as $[bx^k]$, we know from part (b) that $[b] = 0 \Leftrightarrow ba^N = 0$ for large enough N, which is guaranteed by assumption. Therefore $[b] = 0$ for arbitrary $b \in R$ and $[bx^k] = 0$.

    Conversely, if R' is the zero ring, then $1 \in R$ is in the kernel of φ, therefore by part (b), $a^n \cdot 1 = a^n = 0$ for some n.

15. (a) Reduction mod 2: the polynomial becomes $x^3 + x + 1 \in \mathbb{Z}_2[x]$. We can directly check that it has no roots, so it must be irreducible. (If it was reducible, it has contains a degree 1 factor, which means that it has a root.) Irreducibility over $\mathbb{Z}_2$ implies irreducibility over $\mathbb{Q}$.

    (b) Eisenstein's criterion for $p = 3$ gives the desired result, since the top degree coefficient is not divisible by 3, while all other coefficients are. And the constant coefficient is not divisible by 9.

(c) $f(1) = 0 \in \mathbb{Z}_p$, so it must be reducible. Alternatively, one can expand and check that $f(x+1) = x^{p-1} \in \mathbb{Z}_p[x]$.

(d) One can check in $\mathbb{Z}_2[x]$. It has no roots so it cannot have linear factors. So it was reducible, it must be the product of two degree 2 polynomials. But there is only one irreducible degree 2 polynomials over $\mathbb{Z}_2[x]$, which is $x^2 + x + 1$. So if $x^4 - x - 1$ was reducible, it has to be $(x^2 + x + 1)^2$. One can easily check that it gives a contradiction. So $f(x)$ is irreducible in $\mathbb{Z}_2[x]$ and hence in $\mathbb{Q}[x]$.

(e) It is reducible since $(x + iy)(x - iy) = x^2 + y^2 \in \mathbb{C}[x, y]$.

(f) If $f(x, y) = y - x^2$ was reducible, because it is a degree two polynomial, we know $y - x^2 = (a + bx + cy)(d + ex + fy) = ad + bex^2 + cfy^2 + (ae + bd)x + (af + cd)y + (bf + ce)xy$.

Right away we get $ad = cf = ae + bd = bf + ce = 0$. So a or d is 0 and c or f is 0. From $af + cd = 1$, we only have two cases $a = f = 0$ or $c = d = 0$.

In the first case, $a = f = 0$. Since $0 = ae + bd = bd$ and $d \neq 0$, we have $b = 0$. So $bex^2 = 0x^2$, which is a contradiction.

In the second case, $c = d = 0$. Since $0 = ae + bd = ae$ and $a \neq 0$, we must have $e = 0$. So $bex^2 = 0x^2$, which is a contradiction.

Remark: If anything, this highlights how difficult it is to prove whether a polynomial is reducible or not, we are only looking at degree two polynomials in two variables.

16. (a) If -1 is a square in $\mathbb{Z}_p$, say $-1 = a^2$, then we have

$$X^4 + 1 = X^4 - a^2 = (X^2 + a)(X^2 - a).$$

(b) If p is odd and 2 is a square in $\mathbb{Z}_p$, say $2 = b^2$, then we have

$$X^4 + 1 = (X^2 + 1)^2 - (bX)^2 = (X^2 + bX + 1)(X^2 - bX + 1).$$

(c) If p is odd and neither -1 nor 2 is a square, since $\mathbb{Z}_p^\times$ is a cyclic group of even order, we know $-1, 2$ are odd order elements, therefore then their product -2 is an even order element, hence a square, say $-2 = c^2$. Then we have

$$X^4 + 1 = (X^2 - 1)^2 - (cX)^2 = (X^2 - cX - 1)(X^2 + cX - 1).$$