THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 9 Solutions
18th April 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

Compulsory Part

1. Yes. In fact, $F[x]/(x-a) \cong F$ for any $a \in F$. This is due to the first isomorphism theorem, one can define the evaluation map $\phi : F[x] \to F$ by $\phi(f(x)) = f(a)$. This is clearly a surjective ring homomorphism, as $\phi(k) = k$ for any $k \in F$. Therefore, it suffices to show that $\ker \phi = (x-a)$.

   Let $f(x) \in (x-a)$, i.e. $f(x) = (x-a)g(x)$ for some polynomial $g \in F[x]$, then $\phi(f(x)) = f(a) = (a-a)g(a) = 0$, so $f(x) \in \ker \phi$.

   Conversely, let $f(x) \in \ker \phi$, then $f(a) = 0$. Write $f(x) = \sum_{k=0}^{n} c_k x^k = \sum_{k=0}^{n} c_k (x - a + a)^k = \sum_{k=0}^{n} c_k \sum_{i=0}^{k} \binom{k}{i} (x-a)^i a^{k-i} = \sum_{i=0}^{n} (\sum_{k=i}^{n} c_k \binom{k}{i} a^{k-i})(x-a)^i$.

   Now $f(a) = 0$ implies that there is no $i = 0$ term, i.e. the coefficient of $(x-a)^0$ is 0. Therefore $f(x) = \sum_{i=1}^{n} (\sum_{k=i}^{n} c_k \binom{k}{i} a^{k-i})(x-a)^i = (x-a) \cdot \sum_{i=1}^{n} (\sum_{k=i}^{n} c_k \binom{k}{i} a^{k-i})(x-a)^{i-1}$, so $f(x) \in (x-a)$ as desired.

   Since $F[x]/(x-a) \cong F$ regardless of what $a \in F$ is, we have $F[x]/(x-a) \cong F[x]/(x-b)$.

2. (a) Not isomorphic. We can simply consider the additive groups of the quotient rings, which are quotient groups. We will simply show that they have finite but different order, so has no hope of being isomorphic.

   In fact, we will prove something that is more general. Consider F a field, and the principal ideal $(f(x)) \subset F[x]$. The claim is that cosets of $(f(x))$ are represented by polynomials of degree smaller than or equal to $\deg f(x)$. This is simply due to division algorithm, any coset $p(x) + (f(x))$ is equal to some $r(x) + (f(x))$ with $\deg r < \deg f$. And if $r_1 \neq r_2$, then they represent different cosets.

   In our case, this implies that $\mathbb{Z}_2[x]/(x^2+1)$ has order 4 since there are 4 polynomials of degree less than 2, i.e. $0, 1, x$ and $x+1$; and $\mathbb{Z}_2[x]/(x^3+1)$ has cardinality 8 since there are 8 polynomials of degree less than 3, namely $0, 1, x, x+1, x^2, x^2+1, x^2+x$ and x^2+x+1.

   (b) Yes they are isomorphic. Consider $\phi : \mathbb{R}[x] \to \mathbb{R}[x]/(x^2-2x+1)$ by $\phi(x) = x - 1 + ((x^2-2x+1)$. This defines a homomorphism because for any polynomial $p(x) = \sum_{i=0}^{n} a_i x^i$, one can define $\phi(p(x)) = \sum_{i=0}^{n} a_i (x-1)^i + (x^2-2x+1) = p(x-1) + (x^2-2x+1)$. And it is clear that if $f(x) = p(x)q(x)$, then $f(x-1) = p(x-1)q(x-1)$. It suffices to prove that it is surjective and has kernel given by (x^2). Clearly the map is surjective, since any element $f(x) + (x^2-2x+1) \in \mathbb{R}[x]/(x^2-2x+1)$ is the image of $f(x+1)$. Now $\ker \phi$ contains those $f(x) \in \mathbb{R}[x]$ so that $f(x-1) \in (x^2-2x+1)$. This is equivalent to x^2-2x+1 being a factor of $f(x-1)$, hence it is the same as x^2 being a factor of $f(x)$. So $\ker \phi = (x^2)$.

(c) Not isomorphic. In $\mathbb{Q}[x]/(x^2)$ there is a nonzero element that squares to 0, i.e. $x + (x^2)$ satisfies $x^2 + (x^2) = 0$. We claim that such an element does not exist in $\mathbb{Q}[x]/(x^2 - 1)$. If $f(x) + (x^2 - 1)$ squares to 0, then $f(x)^2$ is divisible by $x^2 - 1$. Therefore, $f(x)^2$ is divisible by both $x + 1, x - 1$, so $f(1)^2 = f(-1)^2 = 0$. In particular, $f(1) = f(-1) = 0$ must also be true. Then $f(x)$ is divisible by $x^2 - 1 = (x + 1)(x - 1)$, then $f(x) + (x^2 - 1)$ is simply 0. If the rings were isomorphic, then there the image of $x + (x^2)$ would be a nonzero element that squares to 0, so such an isomorphism does not exist.

(d) They are isomorphic. We have already seen that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ from the lecture. It suffices to do the same for the other ring. Consider $\phi : \mathbb{R}[x] \to \mathbb{C}$ defined by $\phi(x) = \sqrt{2}i$. This clearly defines a ring homomorphism. It is surjective because $\phi(a + bx/\sqrt{2}) = a + bi \in \mathbb{C}$ for arbitrary $a, b \in \mathbb{R}$. It suffices to show that $\ker \phi = (x^2 + 2)$.

If $f(x) \in \ker \phi$, then $f(\sqrt{2}i) = 0$, so that $x - \sqrt{2}i$ is a complex factor of $f(x)$. Now $f(x) \in \mathbb{R}[x]$ implies that $x + \sqrt{2}i$ is another complex factor of $f(x)$, therefore $(x+\sqrt{2}i)(x-\sqrt{2}i) = x^2+2$ is a real factor of $f(x)$, so $f(x) \in (x^2+2)$. Conversely, if $f(x) \in (x^2 + 2)$, clearly $f(\sqrt{2}i) = 0$.

By the first isomorphism theorem, we have $\mathbb{R}[x]/(x^2 + 2) \cong \mathbb{C}$ as desired.

3. (a) Since $\mathbb{Q} \subset \mathbb{C}$, we may realize $\mathbb{Q}[\sqrt{d}]$ is the image of $\mathbb{Q}[x] \to \mathbb{C}$ defined by $x \mapsto \sqrt{d}$, so it is a subring. Being a subring of a field, it is automatically an integral domain, otherwise the existence of zero divisors would contradict to the fact that $\mathbb{C}$ is a field.

(b) For any $\alpha = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, define $\overline{\alpha} = a - b\sqrt{d}$. Note that $\alpha\overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d = N(\alpha) = N(\overline{\alpha})$. Also we have $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$, as $(a - b\sqrt{d})(e - f\sqrt{d}) = ae + bfd - (af + be)\sqrt{d})$, whereas $(a + b\sqrt{d})(e + f\sqrt{d}) = ae + bfd + (af + be)\sqrt{d}$.

Therefore, for any $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$, we have $N(\alpha\beta) = \alpha\beta\overline{\alpha}\overline{\beta} = N(\alpha)N(\beta)$.

Finally, $N(\alpha) = \alpha\overline{\alpha} = 0$ implies that $\alpha = 0$ or $\overline{\alpha} = 0$ as $\mathbb{Q}[\sqrt{d}]$ is an integral domain. If $\overline{\alpha} = a - b\sqrt{d} = 0$ then $a = b = 0$, so $\alpha = 0$ regardless.

(c) From argument similar to Tutorial 9 Q6, $\mathbb{Q}[\sqrt{d}]$ is the smallest subring containing $\mathbb{Q}$ and $\sqrt{d}$. It suffices to check that it is also a field. Indeed, if $a + b\sqrt{d} \neq 0$, then $0 \neq N(\alpha) \in \mathbb{Q}$, so that $x = \overline{\alpha}/N(\alpha)$ satisfies $x\alpha = \alpha\overline{\alpha}/N(\alpha) = 1$. So every nonzero element is invertible.

(d) This is essentially part of part (a), we have a surjective homomorphism $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{d}] \subset \mathbb{C}$. It suffices to verify that $\ker \phi = (x^2 - d)$ and apply the first isomorphism theorem. Let $f(x) \in \ker \phi$, then $f(\sqrt{d}) = 0$, so $x - \sqrt{d}$ is a complex factor of $f(x)$. Now $\sqrt{d} \mapsto -\sqrt{d}$ defines a field automorphism of $\mathbb{Q}[\sqrt{d}]$ which fixes $\mathbb{Q}$, therefore we also have $f(-\sqrt{d}) = 0$ and $x + \sqrt{d}$ is also a complex factor of f. Then $x^2 - d = (x + \sqrt{d})(x - \sqrt{d})$ is a rational factor of $f(x)$, so $f(x) \in (x^2 - d)$.

Conversely if $f(x) = (x^2 - d)p(x)$ for some polynomial p, then clearly $f(\sqrt{d}) = 0$, so $f \in \ker \phi$.

4. (a) The image of $f(x)$ in $\mathbb{Z}_2$ is $\bar{f} = x^3 + x + 1$, note that $\bar{f}(0) = \bar{f}(1) = 1$, so it has no root in $\mathbb{Z}_2$, so it has no linear factor. Therefore it must be irreducible over $\mathbb{Z}_2$, so it is irreducible over $\mathbb{Z}$, so it is irreducible over $\mathbb{Q}$ by Gauss' theorem.

(b) If x^4+x^2+x+1 has a rational root, by proposition 12.1.1, it must be ± 1, clearly both are not roots. Therefore, if it is reducible over $\mathbb{Z}$, it is a product of two irreducible degree 2 factors. Suppose $x^4 + x^2 + x + 1 = (x^2 + ax \pm 1)(x^2 + bx \pm 1) = x^4 + (a+b)x^3 + (ab \pm 2)x^2 + (\pm a \pm b)x + 1$. Therefore $b = -a$, and $-a^2 \pm 2 = 1$, so the only possibility is $a^2 = 1$, and $a = \pm 1$. But then $\pm a \pm b = 0$, this gives a contradiction. Therefore $x^4 + x^2 + x + 1$ is irreducible over $\mathbb{Z}$, so it is irreducible over $\mathbb{Q}$ by Gauss' theorem.

(c) Consider $f(x+1) = 4(x+1)^3 - 6(x+1) - 1 = 4x^3 + 12x^2 + 12x + 4 - 6x - 6 - 1 = 4x^3 + 12x^2 + 6x - 3$. Then 3 is a prime that divide all the non-leading coefficients, and 9 does not divide the constant coefficient -3. Therefore we can apply Eisenstein's criterion to conclude that $f(x+1)$ (and hence $f(x)$) is irreducible over $\mathbb{Z}$. So by Gauss' theorem, it is also irreducible over $\mathbb{Q}$.

Alternatively, one can note that for a cubic polynomial to be reducible, it must have some root in $\mathbb{Q}$. So by proposition 12.1.1, the only possible roots are $\pm 1, \pm\frac{1}{2}$ or $\pm\frac{1}{4}$. Then it is straightforward to check directly that none are actually roots of the polynomial. So it is irreducible over $\mathbb{Q}$.

5. (a) Note that the polynomial $x^{17} + 5x^2 - 10x + 45$ has a prime number 5 that divides all the non-leading coefficients, and 25 does not divide 45. So Eisenstein's criterion implies that it is irreducible. Since $\mathbb{Q}$ is a field, then by theorem 11.1.10 the quotient ring is always a field.

(b) It is not a field. We may take for example the element $2 + (x^6 - 210x - 616) \in \mathbb{Z}[x]/(x^6 - 210x - 616)$ and show that it is not invertible. If it was invertible, then there are polynomials $a(x), b(x) \in \mathbb{Z}[x]$ so that $2a(x) + b(x)(x^6 - 210x - 616) = 1$. Now evaluate this expression at $x = 0$, we get $2a(0) - 616b(0) = 1$. This is a contradiction as the LHS is even and RHS is odd. So $2 + (x^6 - 210x - 616)$ is not invertible in the quotient ring, it cannot be a field.

(c) By Q4c, the polynomial $4x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$. Therefore by theorem 11.1.10, the quotient ring is a field.

(d) Recall that an irreducible polynomial in $\mathbb{R}[x]$ is either of degree 1 or degree 2. Actually in our case, since the degree of the polynomial is odd, by intermediate value theorem, it has a real root α, therefore it has a linear factor $x - \alpha$. Since it is reducible, the quotient ring is not a field.

Optional Part

1. Since f, g are coprime, there are $a, b \in F[x]$ so that $af + bg = 1$ by corollary 11.1.5. And by assumption we have $h = cf = dg$ for some polynomials $c, d \in F[x]$. Therefore $c = c(af + bg) = caf + cbg = dag + cbg = g(da + cb)$. Then simply substitute to obtain $h = cf = fg(da + cb)$. So fg divides h.

2. We may simply perform long division to compute: $g = x^3 - 2x + 1 = (x+1)(x^2 - x - 2) + x + 3$. Set $r_1 = x + 3$, then compute $f = x^2 - x - 2 = (x+3)(x+1) + 0$. Now the remainder is 0. So we may write $g - (x+1)f = x + 3 = \gcd(f, g)$.

3. (a) In $\mathbb{Z}_2[x]$, we have $x^4 + 1 = x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x^2 - 1)(x^2 - 1) = (x+1)^2(x-1)^2 = (x-1)^4$. Clearly the linear factor $x - 1$ is irreducible.

(b) In $\mathbb{Z}_3[x]$, we have $x^3+1 = x^3+3x^2+3x+1 = (x+1)^3$. Clearly $x+1$ is irreducible.

4. (a) Eisenstein's criterion with $p = 5$.

   (b) Consider reduction mod 2, we obtain $x^2 + x + 1$, this does not have a root in $\mathbb{Z}_2$ so it is irreducible over $\mathbb{Z}_2$, so irreducible over $\mathbb{Z}$, hence irreducible over $\mathbb{Q}$ by Gauss' lemma.

   (c) For degree 3, it suffices to check that it has no rational roots, which if exists, must be either ± 1 or ± 7. By direct checking, none of these numbers are actually roots of the polynomial.

   (d) Consider two times the polynomial, whose irreducibility is equivalent. We have $8x^3 - 6x + 1$. Again it suffices to check that it has no roots, which could only be $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ if exist. One can directly check that none are roots.

   (e) Likewise, irreducibility is equivalent to that of x^5-3x^4+3. One can conclude using Eisenstein's criterion with $p = 3$.

   (f) Over $\mathbb{Z}_2$, the polynomial is reduced to $x^4 + x^2 + 1 = x^4 + 2x^2 + 1 - x^2 = (x^2 + x + 1)(x^2 - x + 1)$. The degree two factors are irreducible since it has no roots in $\mathbb{Z}_2$. On the other hand, over $\mathbb{Z}_3$, we get $x^4 + 2x^2 + x = x(x^3 + 2x + 1)$. The degree 3 factor is irreducible as it has no roots in $\mathbb{Z}_3$.

   Now if the original polynomial was reducible over $\mathbb{Z}$. Then taking mod 2 and mod 3 will obtain factorization of the corresponding polynomials as a product of polynomials of the same product types (for example, a product of a degree 2 with another degree 2, etc). Since the irreducible factorization of the polynomial are different in $\mathbb{Z}_2$ and $\mathbb{Z}_3$, it is impossible for the original polynomial to be reducible in $\mathbb{Z}$.

5. We will prove the contrapositive, if f^* is reducible, say $f^* = gh$ for some nonconstant polynomials $g, h \in k[x]$. We claim that $(f^*)^* = f$ and $(gh)^* = g^*h^*$, therefore $f = (f^*)^* = g^*h^*$ implies that f is also reducible, as g^*, h^* are nonconstant polynomials again.

   It suffices to prove the claim, one may write for a degree n polynomial f, $f^*(x) = x^n f(1/x)$. Since f^* is again of degree n, we have $(f^*)^*(x) = x^n(\frac{1}{x})^n f(1/\frac{1}{x}) = f(x)$, as desired.

   Let $\deg g = l, \deg h = m$, so that $\deg(gh) = l + m$, then $(gh)^*(x) = x^{l+m}g(\frac{1}{x})h(\frac{1}{x}) = x^l g(\frac{1}{x})x^m h(\frac{1}{x}) = g^*(x)h^*(x)$, as claimed.

6. (a) No, because $x^3 - 1 = (x - 1)(x^2 + x + 1)$ is reducible.

   (b) Yes, because the polynomial in question is irreducible according to Eisenstein's criterion for prime $p = 3$.

   (c) Yes, the polynomial in question is irreducible as it has no roots. Note that a rational root, if exists, would be ± 1, which clearly are not the roots.

   (d) No, the class represented by 3 is not invertible, indeed if it was invertible then there are polynomials $a(x), b(x) \in \mathbb{Z}[x]$ so that $3a(x)+(x^3+x+1)b(x) = 1$. Substituting $x = 1$, we get $3a(1) + 3b(1) = 1$, clearly the LHS is divisible by 3 but the RHS is not. This gives a contradiction. So 3 is not invertible in the quotient ring.

   (e) No. (17) is the whole field, since for any $q \in \mathbb{Q}$, $q = q/17 \cdot 17 \in (17)$. So the quotient ring is the zero ring, which is not a field.

(f) Yes. As we have seen from the lecture, this is the ring of integers modulo 17, $\mathbb{Z}/17\mathbb{Z}$, which is a field, as any non-zero number has an inverse. (Any number x that is not a multiple of 17 is coprime to 17 so there are $a, b \in \mathbb{Z}$ so that $ax + 17b = 1$ so a is inverse to x modulo 17.

(g) Yes, it is a field. In fact, $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$. To see this, define $\phi : \mathbb{Z}[x] \to \mathbb{Z}_2$ by $\phi(f(x)) = f(0) \bmod 2$. This is clearly a surjective ring homomorphism, so it suffices to check that $\ker \phi = (2, x)$. The inclusion $(2, x) \subset \ker \phi$ is clear. To see $\ker \phi \subset (2, x)$, let $f(x)$ so that $f(0) = 0 \bmod 2$. Then $f(0) = 2k$ for some integer k. So we can write $f(x) = 2k + a_1x + ... + a_nx^n = 2k + x(a_1 + ... + a_nx^{n-1}) \in (2, x)$.

(h) Yes, by compulsory Q3. Or just note that the polynomial is irreducible.

(i) No, $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$, the polynomial is reducible. So the quotient is not a field.

(j) Yes, $x^2 + 3$ is irreducible as $x^2 + 3 > 0$ for any $x \in \mathbb{R}$, so it has no root.

(k) No. In $\mathbb{F}_5$, $2^2 = 4 = -1$, so the polynomial is actually reducible $x^2 + 1 = (x - 2)(x - 3)$. So the quotient is not a field.

(l) No, again an odd degree polynomial has a real root, so it is reducible.

7. Consider the contrapositive, if f is reducible, say $f = ab$ for some nonconstant polynomials $a, b \in F[x]$, then $\deg f > \deg a, \deg b$. We have f divides $f = ab$, but f cannot possibly divide a or b for degree reasons.