THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Tutorial 11 Solutions
15th April 2024

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

1. (a) Regard $f(x) = x^4 + 1$ as a polynomial in $\mathbb{C}[x]$, by the fundamental theorem of algebra, it has 4 roots counting multiplicities. And more generally, given a real polynomial $f(x) \in \mathbb{R}[x]$, if $\alpha \in \mathbb{C}$ is a complex root, then its complex conjugate $\bar{\alpha}$ is also a root, this is because complex conjugation is an automorphism of $\mathbb{C}$ which fixes the subfield $\mathbb{R} \subset \mathbb{C}$, therefore $0 = \overline{f(\alpha)} = \bar{f}(\bar{\alpha}) = f(\bar{\alpha})$, where $\bar{f}$ is the polynomial obtained from taking conjugates of all coefficients.

   Therefore if $\alpha \in \mathbb{C} \setminus \mathbb{R}$, the factor $(x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha + \bar{\alpha}) + \alpha\bar{\alpha}$ divides $f(x)$, and has real coefficients. So it is an irreducible factor. By induction, we see that any real polynomial has irreducible factors of degree 1 or 2.

   In the present case, simply for degree reason, $f(x) = x^4 + 1$ is reducible in $\mathbb{R}[x]$. Specificcally, one may factorize it as $x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2+1)^2 - (\sqrt{2}x)^2 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$. It is simple to see that the quadratic factors are irreducible as they have no real roots.

   (b) Since $\mathbb{Q}[x] \subset \mathbb{R}[x]$, part (a) shows a factorization of $x^4 + 1$ into irreducible in $\mathbb{R}[x]$, which admits unique factorization property. If it was possible to factorize x^4+1 into nontrivial factors over $\mathbb{Q}[x]$, then such a factorization holds also in $\mathbb{R}[x]$. This would contradict unique factorization property. So $x^4 + 1$ must be irreducible in $\mathbb{Q}[x]$.

   (c) The polynomial is irreducible in $\mathbb{Z}[x]$ according to Eisenstein's criterion when applied to the prime 11. So by Gauss' theorem it is irreducible in $\mathbb{Q}[x]$.

   (d) This is a cyclotomic polynomial, its irreducibility over $\mathbb{Z}[x]$ is a consequence of Eisenstein's criterion for the prime 5, so Gauss' theorem implies that it is irreducible over $\mathbb{Q}[x]$.

   (e) A degree 3 polynomial over $F[x]$ where F is a field, is irreducible if and only if it has no linear factor, which is equivalent to that it has not root in F. By proposition 12.1.1, we know that if $x^3 - 7x^2 + 3x + 3$ has a root, then it must be a rational number q that when written in reduced fraction form $q = s/t$, we have s dividing 3 and t dividing 1, therefore $q = \pm 1$ or ± 3. It is clear that by direct checking 1 is a root, therefore it is reducible.

   (f) Similar to previous question, we simply have to check whether $x^3 - 5$ has a root in $\mathbb{Z}_{11}$. Here we compute:

x	0	1	2	3	...
$x^3 - 5$	6	7	3	0	...

   As we see quickly, 3 is a root of $x^3 - 5$, therefore $x - 3$ is a factor. So it is reducible.

(g) A degree 4 polynomial is reducible if and only if it is either a product of two degree 2 irreducibles or it contains a linear factor. As we can compute directly, $f(x) = x^4 + x + 1$ has $f(0) = f(1) = 1$. So it has no roots in $\mathbb{Z}_2$. So it is reducible, it must be a product of degree 2 irreducible polynomials.

Note that the degree 2 polynomials in $\mathbb{Z}_2[x]$ are $x^2, x^2 + 1, x^2 + x, x^2 + x + 1$. It is clear that the first three are all reducible, as they have roots in $\mathbb{Z}_2$. So there is only one irreducible degree 2 polynomial. So if $f(x)$ was reducible, it must be equal to $(x^2 + x + 1)^2$. This computes to $x^4 + x^2 + 1$, which is not equal to $f(x)$. So $f(x)$ is in fact irreducible.

2. Assuming Gauss' theorem, if $f(x) = \sum_{i=0}^{n} a_i x^i$ is a polynomial with integer coefficients, and $q = s/t \in \mathbb{Q}$ is a rational root written in reduced form. Then $x - q$ is a factor of $f(x)$ in $\mathbb{Q}[x]$. Gauss's theorem implies that there is a linear polynomial in $\mathbb{Z}[x]$ that divides $f(x)$. The primitive of $x - q$ is given by $tx - s \in \mathbb{Z}[x]$. Therefore $f(x) = (tx - s)p(x)$ for some $p(x) \in \mathbb{Z}[x]$, from this, it is clear that t divides a_n and s divides a_0.

3. Suppose that $f(x) = x^n + 5x^{n-1} + 3 = g(x)h(x)$ for some polynomials $g, h \in \mathbb{Z}[x]$. Then we denote $\overline{g}, \overline{h}$, etc by the corresponding polynomial in $\mathbb{Z}_3[x]$. We have $x^{n-1}(x+5) = \overline{g} \cdot \overline{h}$. Since $\mathbb{Z}_3[x]$ has unique factorization, we know that without loss of generality, up to units, $\overline{g} = x^i$ and $\overline{h} = x^j(x + 5)$ where $i + j = n - 1$.

   Now notice that if i or j is nonzero, then the constant coefficients of $\overline{g}, \overline{h}$ are 0, therefore the constant coefficients of g, h are divisible by 3. So $f = gh$ has constant coefficient 3 divisible by 9, that is a contradiction. So we must have either $i = 0$ or $j = 0$.

   If $j = 0$, then $\overline{g} = x^{n-1}$ and $\overline{h} = x + 5$. That implies that $h(x)$ is a linear polynomial. Therefore $f(x)$ would have integer roots by proposition 12.1.1, the root if exists must be ± 1 or ± 3. We can directly check that none of these is a root of $f(x)$: $f(1) = 9$, $f(-1) = -1$ when n is even and $f(-1) = 7$ when n is odd; $f(3) > 0$ clearly and $f(-3) = 2(-3)^{n-1} + 3$ is never 0. So it is impossible to have linear factors, and this case is rejected.

   So the only possibility is $i = 0$, in which case $\overline{g} = 1$ and $\overline{h} = x^{n-1}(x + 5)$. So $f(x)$ is irreducible.

4. Suppose that $f(x) = \prod_{k=1}^{n}(x - a_i) - 1$ is reducible over $\mathbb{Q}[x]$, by Gauss lemma it is reducible over $\mathbb{Z}[x]$ as well. Write $f(x) = g(x)h(x)$ for some monic polynomials $g, h \in \mathbb{Z}[x]$, since f is monic, we have $\deg g, \deg h < \deg f$. Note that $f(a_i) = g(a_i)h(a_i) = -1$. Therefore $g(a_i)$ and $h(a_i)$ take values ± 1 with opposite signs. Therefore $g(a_i) + h(a_i) = 0$ for $i = 1, ..., n$. Since $\deg(g+h) \leq \max\{\deg f, \deg g\} < \deg f = n$, according to the fundamental theorem of algebra, it is impossible for a nonzero polynomial of degree less than n having n distinct roots.

   The only possibility is that $g + h = 0$, so n is even and $f(x) = -g(x)^2$. This also leads to a contradiction as the leading coefficient of LHS is 1 and -1 on the RHS. So $f(x)$ must be irreducible.

5. (a) The content of this exercise (and other generalities about Gaussian integers, etc, won't appear in the exams.)

   Recall that in $\mathbb{Z}[i]$, there is a norm function $N(a + bi) := a^2 + b^2$ that satisfies the property that if $a + bi$ divides $c + di$, then $N(a + bi)$ divides $N(c + di)$. We have $2 = (1+i)(1-i) = N(1+i)$. Now $N(z) = 1$ if and only if z is a unit, i.e. $z = \pm 1$ or $\pm i$. So we see that $1+i$ is an irreducible (a prime) in $\mathbb{Z}[i]$. By a generalization of proposition 12.1.1, if $x^4 - 4x + 2$ has a root in $\mathbb{Z}[i]$, it must be $\pm 1, \pm i, \pm(1+i), \pm(1-i), \pm 2$ or $\pm 2i$. Note that for $\pm i, \pm(1+i), \pm(1-i)$ or $\pm 2i$, the x^4 term evaluates to a real number, so they are clearly not roots of $x^4 - 4x + 2$. For $\pm 1, \pm 2$, directly checking also shows that they are not roots.

So if $x^4 - 4x + 2$ is reducible, it must be a product of two degree 2 irreducible polynomials.

(b) Consider now $x^4 - 4x + 2$ over $\mathbb{Z}_5$. Note that 2 is a root, as $2^4 - 8 + 2 = 0 \in \mathbb{Z}_5$. By long division, one calculates $x^4 - 4x + 2 = (x-2)(x^3 + 2x^2 + 4x + 4)$. And $p(x) = x^3 + 2x^2 + 4x + 4$ is irreducible in $\mathbb{Z}_5$ since it has no roots: $p(0) = 4, p(1) = 1, p(2) = 3, p(3) = 1, p(4) = 1$.

(c) Recall that $\mathbb{Z}[i]/(2-i) \cong \mathbb{Z}_5$, so there is a surjective map $\mathbb{Z}[i] \to \mathbb{Z}_5$ by sending $a + bi \mapsto a + 2b \mod 5$. Therefore if $f(x)$ was reducible in $\mathbb{Z}[i]$, it is a product of two degree 2 polynomials, when passed to $\mathbb{Z}_5$, we may write $f(x)$ has a product of two degree 2 polynomials in $\mathbb{Z}_5[x]$ (which may not be irreducible). This is a contradiction, as the factorization types do not agree (it contradicts unique factorization in $\mathbb{Z}_5[x]$.)

6. No. It is not a field in general. For example, for a prime number p, regarded as a constant polynomial, is irreducible in $\mathbb{Z}[x]$. And the quotient ring $\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x]$ is not a field, as $x + (p)$ is not invertible. If $f(x)$ is a higher degree irreducible polynomials in $\mathbb{Z}[x]$. We claim that $\mathbb{Z}[x]/(f(x))$ has characteristic 0, and $n > 1$ is non-invertible in the quotient ring, for some suitable n.

7. No, if they were isomorphic, let $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ be an isomorphism, then $\varphi(\sqrt{2})^2 = \varphi(\sqrt{2}^2) = \varphi(2) = 2$ implies that 2 has a square root in $\mathbb{Q}(\sqrt{3})$ as well. Let $a + b\sqrt{3}$ be a square root, then $(a + b\sqrt{3})^2 = 2$ yields $a^2 + 3b^2 + 2ab\sqrt{3} = 2$ for $a, b \in \mathbb{Q}$. So either a or b is equal to 0, either case is impossible as both 2 and $\frac{2}{3}$ does not have square roots in $\mathbb{Q}$.