Algebra II Assignment 2

Due Friday 25th February 2022

Please attempt all four problems in this assignment and submit your answers (before midnight on Friday 25th February) by uploading your work to the Moodle page. If you have any questions, feel free to email me at adsg@hku.hk.

Problem 1 (Irreducible elements in polynomial rings)**.**

1. Let $R = \mathbb{C}[x]$, and let $f \in R$ be irreducible. Show that $R/(f) \cong \mathbb{C}$.

2. Let $R = \mathbb{R}[x]$, and let $f \in R$ be irreducible. Show that either $R/(f) \cong \mathbb{R}$, or $R/(f) \cong \mathbb{C}$.

Solution. We prove it for part 2, the proof for part 1 being a direct adaptation. The irreducible elements in $\mathbb{R}[x]$ are all, up to multiplication by a unit in $\mathbb{R}$, of the form $f(x) = x - a$ for $a \in \mathbb{R}$ or of the form $x^2 + ax + b$ where $b^2 - 4c < 0$.
Case 1: Let f be a degree 1 irreducible polynomial, say $f(x) = x - a$. Then, define the *evaluation map* $ev_a : \mathbb{R}[x] \to \mathbb{R}$ by $ev_a(r) = r, \forall r \in \mathbb{R}$ and $ev_a(x) = a$. Then, ev_a is clearly a surjective ring homomorphism. By definition, $\mathrm{Ker}(ev_a) = \{f \in \mathbb{R}[x] \mid f(a) = 0\}$, i.e. $\mathrm{Ker}(ev_a) = (x - a)$. Therefore, by the first isomorphism theorem, ${\mathbb{R}[x]}\big/{(x-a)} \cong \mathbb{R}$.
Case 2: Let f be a degree 2 irreducible polynomial, say $f(x) = x^2 + bx + c$ with $b^2 - 4c < 0$. By the fundamental theorem of algebra, f has two complex roots α and $\overline{\alpha}$. Define the *evaluation map* ev_α by $ev_\alpha(r) = r, \forall r \in \mathbb{R}$ and $ev_\alpha(x) = \alpha$. Then, ev_α is a ring homomorphism. Suppose that $\alpha = a_1 + ia_2$ for some $a_1, a_2 \in \mathbb{R}$. Since α is a complex root of f, we know that $a_2 \neq 0$. Then, note that the image of the polynomial $\frac{x-a_1}{a_2} \in \mathbb{R}[x]$ under the map ev_α is i. Then, for any complex number $z = u + iw$, $ev_\alpha(u + w\frac{x-a_1}{a_2}) = z$, and so ev_α is surjective. It is easy to see that the kernel of ev_α is precisely $(x^2 + bx + c)$, and so ${\mathbb{R}[x]}\big/{(x^2+bx+c)} \cong \mathbb{C}$. ■

Problem 2 (Construction of finite fields)**.**

1. Show that $f = x^3 + 2x + 1$ is irreducible in $\mathbb{Z}_3[x]$, and deduce that $\mathbb{Z}_3[x]/(f)$ is a field. How many elements does this field have?

2. Write down the multiplication table for the equivalence classes (in $\mathbb{Z}_3[x]/(f)$) with representatives monic polynomials of degree 2 in $\mathbb{Z}_3[x]$.

Solution. 1.If f is reducible, then by comparing degrees, f must be divisible by a linear factor $x - a, a \in \mathbb{Z}_3$. This is equivalent to saying that f must have a root in $\mathbb{Z}_3$. In this case, note that $f(0) = f(1) = f(2) = 1$, and therefore f is irreducible in $\mathbb{Z}_3[x]$. By a result in the course, this implies that the quotient ring $\mathbb{Z}_3[x]/(f)$ is a field. Note that x^3 and $x + 2$ lie in the same equivalence class in the quotient, i.e. $x^3 + (f) = x + 2 + (f)$.

Therefore, $\mathbb{Z}_3[x]/(f) = \{a_0 + a_1x + a_2x^2 + (f) \mid a_0, a_1, a_2 \in \mathbb{Z}_3\}$. It easy to see that no two such elements lie in the same equivalence class, and therefore $\mathbb{Z}_3[x]/(f)$ has precisely $|\mathbb{Z}_3^3| = 3^3 = 27$ elements.
2. This is a tedious but straightforward computation:

	x^2	x^2+1	x^2+2	x^2+x	x^2+x+1	x^2+x+2	x^2+2x	x^2+2x+1	x^2+2x+2
x^2	x^2+2x	$2x^2+2x$	$2x$	x^2+2	$2x^2+2$	2	x^2+x+1	$2x^2+x+1$	$x+1$
x^2+1		$2x+1$	x^2+2x+2	$2x^2+x+2$	x	x^2+x+1	x	x^2+x+1	$2x^2+x+2$
x^2+2			$2x^2+2x+1$	$2x+2$	x^2+2x+1	$2x^2+2x$	$2x+1$	x^2+2x	$2x^2+2+2$
x^2+x				$2x^2+x+1$	$2x+1$	x^2+1	$2x$	x^2	$2x^2+x$
x^2+x+1					x^2+2	$2x^2+x$	x^2+x	$2x^2+2x+1$	2
x^2+x+2						$2x+2$	$2x$	x^2+2	$2x^2+x+1$
x^2+2x							$2x^2+2$	$2x+2$	x^2+x+2
x^2+2x+1								x^2+x	$2x^2+1$
x^2+2x+2									$2x$

Note that fields are commutative, so this table is symmetric along the diagonal. ■

Problem 3 (Irreducibility tests)**.** Determine whether or not the following polynomials are irreducible over $\mathbb{Q}$:

1. $f(x) = 2x^9 + 12x^4 + 36x^3 + 27x + 6$,
2. $f(x) = x^4 + 25x + 7$,
3. $f(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$.

Solution. 1. It is irreducible by applying Eisenstein's criterion with $p = 3$.
2. By the rational root test, if it has a root over $\mathbb{Q}$, the root is either ± 1 or ± 7. A direct computation shows that none of these are roots of f, and therefore $f(x)$ has no roots in $\mathbb{Q}$. Thus, the only possibility is to factor into two quadratic polynomials. By Gauss's lemma, we can assume that the quadratic polynomials are $x^2 + \alpha x \pm 7$ and $x^2 + \beta x \pm 1$ where $\alpha, \beta \in \mathbb{Z}$. Thus, $\alpha = -\beta$, $\pm(\alpha + 7\beta) = 25$ and $\alpha\beta \pm 8 = 0$, which admits no integral solution. Thus, $f(x)$ is irreducible.
3. By the substitution $y = x - 1$, we get $f(x - 1) = x^4 - 2x + 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion with $p = 2$.
■

Problem 4 (Algebraic integers)**.** Let $\mathbb{Z}[x]$ be the ring of polynomials with integer coefficients. We say that a non-zero polynomial $f \in \mathbb{Z}[x]$ is *monic* if its leading coefficient is equal to 1. We say that $\alpha \in \mathbb{C}$ is an *algebraic integer* if there exists a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.[1] The set

$$\overline{\mathbb{Z}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is an algebraic integer}\},$$

is called the set of algebraic integers. In this problem, we will see that $\overline{\mathbb{Z}}$ is a sub-ring of $\mathbb{C}$.

[1] By the fundamental theorem of algebra, the roots of non-zero polynomials all lie in $\mathbb{C}$.

1. Show that $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. Deduce that $\overline{\mathbb{Z}}$ is not a field.

   Throughout the remainder of this problem, let f, g be two polynomials in $\mathbb{Z}[x]$, say

$$f = a_m x^m + \sum_{i=0}^{m-1} a_i x^i, \quad a_i \in \mathbb{Z}, \quad a_m \neq 0,$$

$$g = b_n x^n + \sum_{i=0}^{n-1} b_i x^i, \quad b_i \in \mathbb{Z}, \quad b_n \neq 0.$$

   Define the *resultant* $R(f,g)$ of f and g to be the determinant $\det \begin{pmatrix} R_f \\ R_g \end{pmatrix}$, where:

$$R_f = \begin{pmatrix} a_0 & a_1 & \cdots & a_{m-1} & a_m & 0 & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{m-1} & a_m & 0 & 0 & \cdots & 0 \\ 0 & 0 & a_0 & a_1 & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ & & & \cdots & & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{m-1} & a_m \end{pmatrix} \in M_{n \times (n+m)}(\mathbb{Z}),$$

$$R_g = \begin{pmatrix} b_0 & b_1 & \cdots & b_{n-1} & b_n & 0 & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{n-1} & b_n & 0 & 0 & \cdots & 0 \\ 0 & 0 & b_0 & b_1 & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ & & & \cdots & & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & a_{n-1} & b_n \end{pmatrix} \in M_{m \times (n+m)}(\mathbb{Z}).$$

   If f has roots $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ in $\mathbb{C}$ and g has roots $\{\beta_1, \beta_2, \cdots, \beta_n\}$ in $\mathbb{C}$, one equivalent definition of $R(f,g)$ is called the *product formula* for the resultant:

$$R(f,g) = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j).$$

2. Compute the resultant $R(f,g)$ for the following:

   (a) $f(x) = x^2 + 2x + 2$ and $g = x^2 - 2$.

   (b) $f(x) = x^2 + ax + b$ and $g = 2x + a$.

   (c) $f(x) = x^3 + ax + b$ and $g(x) = 3x^2 + a$.

3. Suppose that $f \in \mathbb{Z}[x]$ is monic with root α and $g \in \mathbb{Z}[x]$ is monic with root β. One can show (try!) that $P(z) := R(f(x), g(z-x)) \in \mathbb{Z}[z]$ is a non-zero monic polynomial with $z = \alpha + \beta$ as a root, and $Q(z) := R(f(x), x^n g(\frac{z}{x})) \in \mathbb{Z}[z]$ is a non-zero monic polynomial with $z = \alpha\beta$ as a root. For each of following pairs of α and β,

   (a) $\alpha = 1 + i$ and $\beta = \sqrt{2}$,

(b) $\alpha = \sqrt{2}$ and $\beta = i\sqrt{3}$,

construct a polynomial with $\alpha + \beta$ as a root and a polynomial with $\alpha\beta$ as a root.

Solution. 1. Since the polynomials $\{x - a \mid a \in \mathbb{Z}\}$ are all monic polynomials in $\mathbb{Z}[x]$, $\mathbb{Z} \subset \overline{\mathbb{Z}}$. Suppose that $\frac{p}{q} \in \mathbb{Q}$ with $\gcd(p, q) = 1, q \neq 1$, is an algebraic integer. Then, there exists $f \in \mathbb{Z}[x]$ monic such that $f(\frac{p}{q}) = 0$. Considering $\mathbb{Z}[x]$ as a subset of $\mathbb{C}[x]$, we factor f as

$$f(x) = (x - \frac{p}{q})(x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0), \quad a_i \in \mathbb{C}.$$

Expanding this expression, the assumption that $f \in \mathbb{Z}[x]$ implies that $a_{n-2} \in q\mathbb{Z}$ and $a_{n-2} - \frac{p}{q} \in \mathbb{Z}$. These facts together imply that q divides p, which is a contradiction. Therefore, the only rational numbers that are algebraic are the integers. Since any field which contains the integers must also contain the rationals, we deduce that $\overline{\mathbb{Z}}$ is not a field.

2(a). The resultant is obtained by taking the determinant of the 4×4 matrix

$$\begin{pmatrix} 2 & 2 & 1 & 0 \\ 0 & 2 & 2 & 1 \\ -2 & 0 & 1 & 0 \\ 0 & -2 & 0 & 1 \end{pmatrix}$$

Explicitly, $R(f, g) = -4$.
2(b). $R(f, g) = 4b - a^2$.
2(c). $R(f, g) = 27b^2 + 4a^3$.

3(a). $1 + i$ and $\sqrt{2}$ are roots of the polynomials in part 2(a). By a direct computation, $g(z-x) = x^2 - 2zx + (z^2 - 2)$, and so $P(z) = z^4 + 4z^3 + 4z^2 + 8$. Similarly, $x^2 g(\frac{z}{x}) = z^2 - 2x^2$ and so $Q(z) = z^4 + 16$.
3(b). The element $\alpha = \sqrt{2}$ is a root of $f(x) = x^2 - 2$, and the element $\beta = i\sqrt{3}$ is a root of $g(x) = x^2 + 3$. Then, $P(z) = z^4 + 2z^2 + 25$ and $Q(z) = (z^2 + 6)^2$. ■