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 $R/(f) \cong \mathbb{C}$.

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 $\mathbb{Z}_3[x]$.

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. $f(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$.

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

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

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.