# MATH 3032: Abstract Algebra

Assignment 2

due 3 February 2023, end of day

Homework should be submitted as a single PDF attachment to `theojf@dal.ca`. Please be sure to include your surname in the file name.

You are encouraged to work with your classmates, but your writing should be your own. If you do work with other people, please acknowledge (by name) whom you worked with.

1. Let $\mathbb{Z}[\sqrt{-5}]$ denote the unital subring of $\mathbb{C}$ consisting of those complex numbers $a + b\mathbf{i}$ such that $a \in \mathbb{Z}$ and $b \in \sqrt{5}\mathbb{Z}$. Said differently, $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \text{ s.t. } a, b \in \mathbb{Z}\}$.

   (a) Describe the ideal $(2) \subset \mathbb{Z}[\sqrt{-5}]$: for which integers $a, b$ is $a + b\sqrt{-5} \in (2)$?

   (b) Describe the ideal $(1+\sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$: for which integers $a, b$ is $a+b\sqrt{-5} \in (1+\sqrt{-5})$?

   Recall that the *norm* of a complex number $z$ is $N(z) = z\bar{z}$, i.e. $N(a + b\mathbf{i}) = a^2 + b^2$. Recall also that that $N(zw) = N(z)N(w)$ for all complex numbers $z, w$.

   (c) Show $N(z) \in \mathbb{Z}$ whenever $z \in \mathbb{Z}[\sqrt{-5}]$. Conclude that if $N(w) = n$, then $N(z) \in n\mathbb{Z}$ for all elements of the principle ideal $(w) \subset \mathbb{Z}[\sqrt{-5}]$. In particular, conclude that $N(z) \in 4\mathbb{Z}$ whenever $z \in (2)$ and that $N(z) \in 6\mathbb{Z}$ whenever $z \in (1 + \sqrt{-5})$.

   (d) Show that if $z, w \in \mathbb{Z}[\sqrt{-5}]$, then $N(z + w) = N(z) + N(w) \mod 2$. Conclude that the ideal $(2, 1 + \sqrt{-5}) = (2) + (1 + \sqrt{-5})$ is not the whole ring $\mathbb{Z}[\sqrt{-5}]$.

   (e) Show that there does not exist an element $z \in \mathbb{Z}[\sqrt{-5}]$ such that $N(z) = 2$.

   (f) Explain this implies that the ideal $(2, 1 + \sqrt{-5})$ cannot be principal.

   (g) Show that there are ring isomorphisms

   $$\mathbb{Z}[\sqrt{-5}]/(1 + \sqrt{-5}) \cong \mathbb{Z}_6, \quad \text{and} \quad \mathbb{Z}[\sqrt{-5}]/(2, 1 + \sqrt{-5}) \cong \mathbb{Z}_3.$$

   Let $\mathbb{Z}_2[\varepsilon]/(\varepsilon^2)$ denote the ring consisting of the four elements $\{0, 1, \varepsilon, 1+\varepsilon\}$, with $1+1 = 0$ and $\varepsilon^2 = 0$ (and of course 0 is the zero element, 1 is the multiplicative unit, etc.). Show that there is a ring isomorphism

   $$\mathbb{Z}[\sqrt{-5}]/(2) \cong \mathbb{Z}_2[\varepsilon]/(\varepsilon^2).$$

2. The *Hurwitz quaternions* are $H := \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H} \text{ s.t. all } a, b, c, d \in \mathbb{Z} \text{ or all } a, b, c, d \in \mathbb{Z} + \frac{1}{2}\}$. For example, $\mathbf{i} - 2\mathbf{j}$ and $\frac{1}{2} + \frac{3}{2}\mathbf{i} - \frac{7}{2}\mathbf{j} - \frac{5}{2}\mathbf{k}$ are elements of $H$ but $\frac{3}{2}\mathbf{i}$ is not.

   (a) Show that $H$ is a (noncommutative!) unital subring of the quaternions $\mathbb{H}$.

   Recall that the *norm* of a quaternion $z$ is $N(z) = z\bar{z}$, i.e. $N(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}) = a^2+b^2+c^2+d^2$.

   (b) Show that $N(zw) = N(z)N(w)$ for all $z, w \in \mathbb{H}$.

(c) Show that $N(z) \in \mathbb{Z}$ for all $z \in H$.

(d) Conclude that an element $z \in H$ is invertible if and only if $N(z) = 1$. Describe the group of units $H^\times$. In particular, what are its elements, and how many are there?

(e) Show that the subset $J \subset H$ defined by

$$J := \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H} \text{ s.t. all } a, b, c, d \in \mathbb{Z} \text{ and } a + b + c + d \in 2\mathbb{Z}\}$$

is a two-sided ideal.

(f) Calculate the quotient ring $H/J$. **Hint:** Show that $|H/J| = 4$. Show that $H/J$ has characteristic 2. Show that $H/J$ contains an element $\omega \neq 1$ such that $\omega^3 = 1$. Conclude that $H/J$ is the finite field $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$.