

Exercise Sheet 2

Algebraic Number Theory

September 23, 2025

Exercises 1, 2, 3 are from Exercise Sheet 1 and they are still relevant for the second week.

Exercise 4 is new.

Exercise 1. Let $j := (-1 + i\sqrt{3})/2 = e^{2i\pi/3}$.

1. Show that $\mathbb{Z}[j]$ is an Euclidean ring and thus principal.
2. Let $p \geq 2$ be a prime number. Prove that we have a ring isomorphism

$$\mathbb{Z}[j]/(p) \cong \mathbb{F}_p[X]/(X^2 + X + 1).$$

3. Deduce that $p \geq 5$ is not prime in $\mathbb{Z}[j]$ if and only if -3 is a square modulo p .
4. Show that -3 is a square modulo p if and only if $p \equiv 1 \pmod{3}$.
Hint: If -3 is a square mod p , construct an element of order 3 in \mathbb{F}_p^\times .
5. Conclude that a prime $p \geq 5$ is of the form $a^2 - ab + b^2$ with $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{3}$.

Exercise 2. Let \mathbb{F} be a field of characteristic $\neq 2$. We define the ring of quaternions over \mathbb{F} , denoted by $\mathbb{H}_{\mathbb{F}}$, as the vector space over \mathbb{F} given by

$$\mathbb{H}_{\mathbb{F}} = \mathbb{F} \oplus \mathbb{F}i \oplus \mathbb{F}j \oplus \mathbb{F}k,$$

together with the ring structure given by

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji \quad \text{and} \quad k = ij.$$

1. For $q = x + yi + zj + wk$, we define $\bar{q} := x - yi - zj - wk$. Prove that

$$\overline{q_1 + q_2} = \bar{q}_1 + \bar{q}_2 \quad \text{and} \quad \overline{q_1 q_2} = \bar{q}_2 \bar{q}_1.$$

2. For $q \in \mathbb{H}_{\mathbb{F}}$, we define the norm of q as $\text{Nr}(q) := q\bar{q}$. Prove that

$$\text{Nr}(q) = x^2 + y^2 + z^2 + w^2 \in \mathbb{F} \quad \text{and} \quad \text{Nr}(q_1q_2) = \text{Nr}(q_1)\text{Nr}(q_2).$$

3. Show that $\mathbb{H}_{\mathbb{F}}$ is a division ring if and only if the norm map $\text{Nr} : \mathbb{H}_{\mathbb{F}} \rightarrow \mathbb{F}$ is non-degenerate, i.e. if $\text{Nr}(q) = 0 \Leftrightarrow q = 0$.

4. Let $p \neq 2$ be a prime. Show that $\mathbb{H}_{\mathbb{F}_p}$ is not a division ring.

Hint: Prove that the two sets $A = \{x^2 + 1 : x \in \mathbb{F}_p\}$ and $B = \{-z^2 : z \in \mathbb{F}_p\}$ satisfy $A \cap B \neq \emptyset$.

Exercise 3. Let $\mathbb{H} \subset \mathbb{H}_{\mathbb{Q}}$ be defined by

$$\mathbb{H} := \{(a + bi + cj + dk)/2 : a, b, c, d \in \mathbb{Z}, a \equiv b \equiv c \equiv d \pmod{2}\}.$$

1. Show that \mathbb{H} is a subring of $\mathbb{H}_{\mathbb{Q}}$ and that $\text{Nr}(\mathbb{H}) \subset \mathbb{N}$. This ring is called Hurwitz's ring.

2. Prove that \mathbb{H} is a (non-commutative) Euclidean ring: For every $x, y \in \mathbb{H}$ with $y \neq 0$, there exists $z, w \in \mathbb{H}$ such that $x = yz + w$ and $\text{Nr}(w) < \text{Nr}(y)$. (This implies in particular that every left/right ideal is principal.)

3. For every $z \in \mathbb{H}$, we have $\text{Nr}(z) = 1 \Leftrightarrow z \in \mathbb{H}^{\times}$.

4. Let $p \neq 2$ be a prime. Prove that there is a ring isomorphism

$$\mathbb{H}/p\mathbb{H} \cong \mathbb{H}_{\mathbb{F}_p},$$

and conclude that there exists $x \in \mathbb{H}$ such that $\text{Nr}(x) = p$. [*Hint:* Use 4(d) to conclude that $p\mathbb{H}$ is not a right maximal ideal in \mathbb{H} .]

5. Let p be an arbitrary prime. First prove that $4p$ can be written as a sum of four squares, and then use this to show that also $2p$ can be written as a sum of four squares.

Hint:

$$\frac{1}{2}(a^2 + b^2 + c^2 + d^2) = \left(\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 \right)$$

6. Prove that every prime p is a sum of four squares. Conclude that for every positive integer n there exist a, b, c, d such that

$$n = a^2 + b^2 + c^2 + d^2.$$

Exercise 4. The goal of this exercise is to prove Fermat's Theorem for $n = 4$: if $(x, y, z) \in \mathbb{Z}^3$ is a solution of

$$X^4 + Y^4 = Z^4, \tag{1}$$

then $xyz = 0$. We do this by contradiction: suppose that (x, y, z) is a solution of (1) and $x, y, z \neq 0$.

1. Show that we can assume that $0 < x, y, z$, $(x, y) = 1$, x odd and y is even.
2. Show that there exist integers $0 < n < m$ such that $(m, n) = 1$, $x^2 = m^2 - n^2$, $y^2 = 2mn$ and n is even.
3. Show that both m and $\frac{n}{2}$ are square numbers.
4. Show that there exists r, s with $(r, s) = 1$, $m = r^2 + s^2$ and $n = 2rs$. Conclude that both r, s are square numbers and that there exist u, v, w such that

$$w^2 = u^4 + v^4$$

and $0 < w < z$.

5. Deduce the desired contradiction.