8. Algebraic numbers: Quadratic fields

Any field of the form $\mathbb{Q}(\sqrt{A})$ where $A \neq 0, 1$ is a square-free integer is said to be a *quadratic field*. A quadratic field $\mathbb{Q}(\sqrt{A})$ is *real* or *imaginary*, according as $A > 1$ or $A < 0$.

Since $\sqrt{A}$ is a root of an irreducible quadratic, $\mathbb{Q}(\sqrt{A})$ consists of the numbers

$$p + q\sqrt{A}, \qquad p, q \in \mathbb{Q}, \tag{1}$$

which satisfy the following properties:

$$(p + q\sqrt{A}) + (r + s\sqrt{A}) = (p + r) + (q + s)\sqrt{A}, \tag{2}$$

$$(p + q\sqrt{A})(r + s\sqrt{A}) = (pr + qsA) + (ps + qr)\sqrt{A}, \tag{3}$$

$$(p + q\sqrt{A})^{-1} = \frac{1}{p^2 - q^2A}(p - q\sqrt{A}). \tag{4}$$

Note that if $p^2 - q^2A = 0$, then either $p = q = 0$ or $q \neq 0$. In the latter case $A = \frac{p^2}{q^2}$ or $\sqrt{A} = \frac{p}{q}$ which is a contradiction. Thus $p^2 - q^2A \neq 0$ unless $p + q\sqrt{A} = 0$ which is equivalent to $p = q = 0$, and the inverse (4) exists for every non-zero quadratic irrationality (1). This number deserves a special notation and for $\alpha = p + q\sqrt{A}$ we denote $N(\alpha) = p^2 - q^2A$ and call the *norm* of α. The norm $N(\alpha)$ of a number $\alpha = (a + b\sqrt{A}) \in \mathbb{Q}(\sqrt{A})$ is the product of α and its *conjugate* $\bar{\alpha} = (a - b\sqrt{A})$, that is, $N(\alpha) = \alpha\bar{\alpha} = (a^2 - b^2A)$.

Proposition 8.13 *The mapping $a + b\sqrt{A} \mapsto a - b\sqrt{A}$, which assigns to each number of $\mathbb{Q}(\sqrt{A})$ its conjugate is an isomorphism of $\mathbb{Q}(\sqrt{A})$ that leaves $\mathbb{Q}$ invariant. α and $\bar{\alpha}$ have the same minimal polynomial.*

Proposition 8.14 *The set of algebraic integers of the field $\mathbb{Q}(i)$ is the set of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.* □

Proposition 8.15 *Let $A > 0$. All the numbers of the form $a + b\sqrt{A}$ with $a, b \in \mathbb{Z}$ are algebraic integers of $\mathbb{Q}(\sqrt{A})$. These are the only integers of $\mathbb{Q}(\sqrt{A})$ if $A \equiv 2$ or $3 \pmod 4$. If $A \equiv 1 \pmod 4$, the numbers $(a + b\sqrt{A})/2$ with odd $a, b \in \mathbb{Z}$ are also integers of $\mathbb{Q}(\sqrt{A})$, and there are no further integers.* □

Exercise 8.6 *Prove Proposition 8.15.*

Proposition 8.16 *For any $\alpha, \beta \in \mathbb{Q}(\sqrt{A})$ we have $N(\alpha\beta) = N(\alpha)N(\beta)$, and $N(\alpha) = 0$ if and only if $\alpha = 0$. For an algebraic integer $\gamma \in \mathbb{Q}(\sqrt{A})$ we have $N(\gamma) \in \mathbb{Z}$, and $N(\gamma) = \pm 1$ iff γ is a unit.* □

Exercise 8.7 *Prove Proposition 8.16.*

Proposition 8.17 *An imaginary quadratic field $\mathbb{Q}(\sqrt{A})$ has units ± 1, and these are the only units except when $A = -1$ (units ± 1 and $\pm i$) and $A = -3$, with units ± 1 and $(\pm 1 \pm \sqrt{-3})/2$.* □

Exercise 8.8 *Prove Proposition 8.17.*

In sharp contrast with the above, for real fields we have:

Theorem 8.18 *There are infinitely many units in any real quadratic field.*

Proof. *It is sufficient to show that for any square-free $A > 1$ the equation $x^2 - Ay^2 = 1$ (called, by mistake,* Pell's equation*) has infinitely many integral solutions. We just give a sketch of the proof here:*

1. *For any $\xi \in \mathbb{R} \setminus \mathbb{Q}$ there are infinitely many $x/y \in \mathbb{Q}$, $(x, y) = 1$, such that $|x/y - \xi| < 1/y^2$.*

2. *For any square-free $A > 1$ there is an k such that $|x^2 - Ay^2| = k$ for infinitely many $x, y \in \mathbb{Z}$.*

3. *For any square-free $A > 1$ the equation $x^2 - Ay^2 = 1$ has an integral solution.*

4. *Prove that there is a solution (x_1, y_1) of $x^2 - Ay^2 = 1$ such that every solution has the form $\pm(x_n, y_n)$ where $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$ for any $n \in \mathbb{Z}$.* □

For the full proof see handout "Pell's equation."

A non-unit algebraic integer $\alpha \in \mathbb{Q}(\sqrt{A})$ is called irreducible *if every algebraic integer that is a divisor of u is either an associate of u or a unit.*

Theorem 8.19 *Every non-unit algebraic integer $\neq 0$ in $\mathbb{Q}(\sqrt{A})$ factors into a product of irreducibles.*

Proof. *Let u be an algebraic integer in $\mathbb{Q}(\sqrt{A})$. Then by Proposition 8.14 $N(u)$ is a rational integer. If u is not irreducible, then $u = vw$, where v, w are algebraic integers and none of them is a unit. Hence $N(v) < N(u)$ and $N(w) < N(u)$ and the proof can be completed by induction on $N(u)$.* □

The decomposition in Theorem 8.19 may not be unique. For example, in $\mathbb{Q}(\sqrt{6})$ we have

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$$

and it is possible to show that all four numbers $2, 5, 2 \pm \sqrt{-6}$ are irreducible.

Lemma 8.20 *(Division algorithm) Let $\alpha \neq 0$ and β be two Gaussian integers. Then there exist Gaussian integers γ and ρ such that $\beta = \gamma\alpha + \rho$ and $N(\rho) < N(\alpha)$.*

Proof. *Let $\beta/\alpha = x + iy$, where x and y are real numbers. Let u and v be, respectively, two integers closest to x and y (these may not be uniquely determined). Define $\gamma = u + iv$, and set $\rho = \beta - \gamma\alpha$. We have to verify that $N(\rho) < N(\alpha)$. Since $\beta = (x + iy)\alpha$, we have*

$$\rho = \beta - \gamma\alpha = (x + iy)\alpha - (u + iv)\alpha = ((x - u) + i(y - v))\alpha.$$

But $|x - u| \leq \frac{1}{2}$ and $|y - v| \leq \frac{1}{2}$, from which

$$N((x - u) + i(y - v)) \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

Therefore, $N(\rho) \leq \frac{1}{2}N(\alpha)$ and the result follows. □

Using this division algorithm, it is possible to develop for Gaussian numbers all standard theory: greatest common divisor, uniqueness of factorisation into irreducibles, etc.

Exercise 8.9 *Check that the proofs given for rational integers work for Gaussian numbers.*

It is known that the only $A < 0$ for which $\mathbb{Q}(\sqrt{A})$ has unique factorisation are $-A = 1, 2, 3, 7, 11, 19, 43, 67,$ and 163.