Algebraic integers

Padmavathi Srinivasan

Week 3

Recall that we defined the height of a point $P = [x_0 : x_1 : \ldots : x_n]$ of $\mathbb{P}^n(\mathbb{Q})$ by first saying that every point of $\mathbb{P}^n(\mathbb{Q})$ has a representative where the x_i are in $\mathbb{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$, and defined $H(P) = \max(|x_0|, |x_1|, \ldots, |x_n|)$. To extend this definition to points of $\mathbb{P}^n(K)$ for a number field K, we first need an analogue of the integers inside a general number K. We will continue using Matt Baker's course notes as a reference – we encourage the interested reader to take a look at his book for proofs.

Definition 1. Let K be a number field. An algebraic integer in K is an element whose minimal polynomial $f(x) := a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$ has $a_0 = 1$ (i.e. f is a monic integral polynomial). The collection of all algebraic integers in K is denoted $\mathcal{O}_K$ and is called the ring of integers of K.

As a sanity check, we first observe that an algebraic integer in $\mathbb{Q}$ is just an integer in $\mathbb{Z}$ – this follows because the minimal polynomial of a rational number a/b written in lowest form with $b > 0$ is $bx - a$, which is monic precisely when a/b is an integer. More generally, the minimal polynomial of an algebraic number α with conjugates $\alpha_1, \alpha_2, \ldots, \alpha_n$ in $\mathbb{C}$ is a multiple of the polynomial $(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) \in \mathbb{Q}[x]$. This easily lets us test if a given algebraic number is an algebraic integer. For instance, if d is a squarefree integer, then one can compute that the minimal polynomial f_α of $\alpha := (1 + \sqrt{d})/2$ in $\mathbb{Q}(\sqrt{d})$ is

$$f_\alpha(x) = \begin{cases} x^2 - x + \frac{1-d}{4} & \text{if } d \equiv 1 \mod 4 \\ 2x^2 - 2x + \frac{1-d}{2} & \text{if } d \equiv 3 \mod 4 \\ 4x^2 - 4x + 1 - d & \text{if } d \equiv 2 \mod 4 \end{cases} \tag{1}$$

This means $(1 + \sqrt{d})/2$ is an algebraic integer precisely when $d \equiv 1 \mod 4$.

Suggested exercises 2. Prove that for every element algebraic number α, there is a nonzero integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.

Fact 1. [Bak22, Chapter 1, Corollary 1.11] *The set $\mathcal{O}_K$ is a subring of K.*

This tells us that we can generate more algebraic integers from known ones by taking sums and products. For example if $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$, then $\sqrt{7} + \sqrt{10}$ is also an algebraic integer – we don't have to write down its minimal polynomial explicitly and check that it is monic! In fact, this tells us that

$$\{a + b(\sqrt{7} + \sqrt{10}) + c(\sqrt{7} + \sqrt{10})^2 + d(\sqrt{7} + \sqrt{10})^3 \ : \ a, b, c, d \in \mathbb{Z}\} \subset \mathcal{O}_K.$$

In particular $\mathcal{O}_K$ is a torsion-free abelian group. We can now ask for the structure of $\mathcal{O}_K$ as an abelian group – is it finitely generated, and if so, what is its rank?

Fact 2. [Bak22, Chapter 1, Theorem 1.18] *As an abelian group $\mathcal{O}_K$ is isomorphic to $\mathbb{Z}^n$, where $n = [K : \mathbb{Q}]$.*

Definition 3. A basis for $\mathcal{O}_K$ as a free $\mathbb{Z}$-module is called an integral basis of K.

Suggested exercises 4.

(a) Prove that if I is a nonzero ideal of $\mathcal{O}_K$, then there is a nonzero integer m in $I \cap \mathbb{Z}$.

(b) Show that every nonzero ideal I is a sublattice of $\mathcal{O}_K$ of maximal rank, i.e. I has finite index in $\mathcal{O}_K$, and is isomorphic to $\mathbb{Z}^n$ as an abelian group.

Visualizing the ring of integers

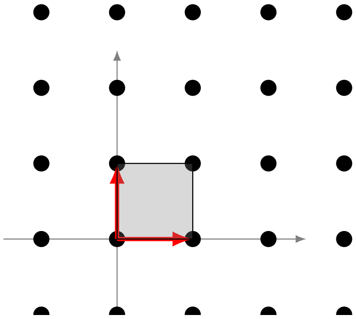
Minkowski introduced beautiful lattice theoretic techniques (colloquially known as geometry of numbers) for understanding the structure of the ring of integers of a number field. If K is a degree n number field, it is possible to view $\mathcal{O}_K$ as an n-dimensional lattice embedded inside n-dimensional Euclidean space $\mathbb{R}^n$. Concretely, we may achieve this by studying the factorization of the minimal polynomial $f \in \mathbb{Z}[x]$ of a primitive element α for K over $\mathbb{R}$. We already saw that over $\mathbb{C}$, the polynomial f splits into n distinct linear factors over $\mathbb{C}$. Suppose that the irreducible polynomial f factors in $\mathbb{R}[x]$ into r linear factors and s quadratic factors. Then $r + s = 2n$, and the n-embeddings of K into $\mathbb{C}$ naturally split into r real embeddings $\sigma_1, \sigma_2, \dots, \sigma_r \colon K \to \mathbb{R}$ and s pairs $(\tau_1, \overline{\tau_1}), (\tau_2, \overline{\tau_2}), \dots, (\tau_s, \overline{\tau_s})$ of complex conjugate embeddings $K \to \mathbb{C}$. (Here for each i between 1 and s, the embedding $\overline{\tau_i}$ is the one obtained by composing the embedding $\tau_i \colon K \to \mathbb{C}$ with complex conjugation.)

Minimal polynomial	**Number field**	**Degree**	**Number of real embeddings**	**Number of pairs of complex conjugate embeddings**
$bx - a$	$\mathbb{Q}$	1	1	0
$x^2 + 1$	$\mathbb{Q}[i]$	2	0	1
$x^2 - 2$	$\mathbb{Q}[\sqrt{2}]$	2	2	0
$x^3 - 2$	$\mathbb{Q}[\sqrt[3]{2}]$	3	1	1
$\varphi_p(x),\ p \geq 3$ prime	$\mathbb{Q}[\zeta_p]$	$p - 1$	0	$(p-1)/2$

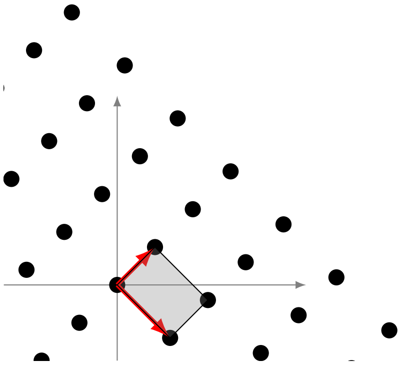
For a complex number $z = a + ib$, let $\mathrm{Re}(z) = a$ denote its real part, and $\mathrm{Im}(z) = b$ denote its imaginary part. The Minkowski embedding $K \to \mathbb{R}^n$ is given by

$$\begin{aligned} &K \to \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^{r+2s} \\ &\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \dots, \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha))), \end{aligned}$$

Fact 3. [Bak22, Chapter 3, Proposition 3.1] *The image of $\mathcal{O}_K$ under the Minkowski embedding is a rank n lattice in $\mathbb{R}^n$.*



Visualizing the ring of integers of $\mathbb{Q}(\sqrt{-1})$ as a lattice



Visualizing the ring of integers of $\mathbb{Q}(\sqrt{2})$ as a lattice

Suggested exercises 5. Verify that $\sqrt{2}+1$ is a unit in the ring $\mathbb{Z}[\sqrt{2}]$. Show that it has infinite order in the group of units of $\mathbb{Z}[\sqrt{2}]$.

1 Computing an integral basis

It is natural to wonder if there is an analogue of the primitive element theorem for the ring of integers of a degree n number field, i.e. if there is an algebraic integer α in K with minimal polynomial f such that $\mathcal{O}_K = \mathbb{Z}[\alpha] := \mathbb{Z}[x]/(f(x))$, or equivalently that there is an integral basis of the form $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ for some $\alpha \in \mathcal{O}_K$ (a "power basis"). For example, we can show that the powers of the element $\alpha := \sqrt{7} + \sqrt{10}$ span the biquadratic field $K := \mathbb{Q}(\sqrt{7}, \sqrt{10})$ as a $\mathbb{Q}$ vector space – one can ask if it is also true that the $\mathbb{Z}$ span of the powers of α equals $\mathcal{O}_K$? Unfortunately, the answer is no. Even worse, we have the following statement.

Example 6 ([Bak22][Chapter 4, Theorem 4.41).] The ring of integers of the biquadratic field $K := \mathbb{Q}(\sqrt{7}, \sqrt{10})$ does not have a power basis, i.e., there is *no algebraic integer* α in this degree 4 number field such that $\{1, \alpha, \alpha^2, \alpha^3\}$ is an integral basis. In fact, one can prove that if α is any algebraic integer in K such that $K = \mathbb{Q}(\alpha)$, then the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ is divisible by 3.[1]

If $\mathcal{O}_K$ has a power basis, then we say that the number field K is monogenic. As the example above illustrates, not all number fields are monogenic – one of the indications that the ring of integers are more subtle than number fields. Nevertheless, there are computational tools for writing down an integral basis.

It is easy to generate a finite index subgroup of $\mathcal{O}_K$ – we can multiply a primitive element for K by a suitable integer and make a new primitive element that is also an *algebraic integer* (do exercise 2!). The subring of $\mathcal{O}_K$ generated by this element has rank $[K : \mathbb{Q}]$ and by Fact 1 has finite index in $\mathcal{O}_K$. In the examples below, let $f(x)$ be a monic irreducible polynomial

[1] One can explain the lack of a power basis in this example by studying ramification of prime ideals in $\mathcal{O}_K$ – a topic covered in a first course in algebraic number theory. Quantifying the proportion of non monogenic number fields of a given degree is an active area of research today!

in $\mathbb{Z}[x]$ with root α and let $K = \mathbb{Q}(\alpha)$. Let m be the index of the finite index subgroup $\mathbb{Z}[\alpha]$ of $\mathcal{O}_K$.

1.1 Index bounds using the discriminant

Our first tool, the discriminant, helps us give explicit upper bounds for the index of a subgroup of $\mathcal{O}_K$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the n embeddings of the degree n number field K in $\mathbb{C}$.

Definition 7. Let $\beta_1, \beta_2, \ldots, \beta_n$ be n algebraic integers of $\mathcal{O}_K$. Let M be the $n \times n$ matrix whose ij-th entry is $\sigma_i(\beta_j)$. Define the associated discriminant by

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) := \det(M)^2 = \det(\sigma_i(\beta_j))^2.$$

Fact 4. [Bak22, Lemma 2.2]

(a) *The discriminant attached to any n algebraic integers of $\mathcal{O}_K$ is an integer.*

(b) *Any two integral bases for $\mathcal{O}_K$ have the same discriminant.*

Definition 8. The discriminant attached to any integral basis is called the discriminant Δ_K of the number field K.

The discriminant of a number field has a geometric interpretation. Recall that every rank n lattice in $\mathbb{R}^n$ with $\mathbb{Z}$-basis $v_1, v_2, \ldots, v_n$ has an associated fundamental domain, which is the region

$$\left\{ \sum_i m_i v_i \ : \ 0 \leq m_i \leq 1 \text{ for all } i. \right\}$$

Suggested exercises 9. Prove that the volume of a fundamental domain for the rank n lattice spanned by the images of $\beta_1, \beta_2, \ldots, \beta_n$ under the Minkowski embedding is $2^{-s}\sqrt{|\Delta(\beta_1, \beta_2, \ldots, \beta_n)|}$.

Suggested exercises 10.

(a) If α is an algebraic integer with minimal polynomial f of degree n, prove that the discriminant of the power basis generated by α is precisely the discriminant of the polynomial f, and we have $\Delta(\alpha) := \Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i)$. In particular, if $f(x) = x^2 + ax + b$, then the corresponding discriminant is $b^2 - 4a$ and if $f(x) = x^3 + ax + b$, then the corresponding discriminant is $-4a^3 - 27b^2$.

(b) Let p be a prime and let φ_p be the p-th cyclotomic polynomial. Show that the discriminant of the power basis generated by a primitive p-th root of unity ζ_p is p^{p-1}. (Hint: Use the equality $\varphi_p(x)(x-1) = x^p - 1$ and the product rule of differentiation to simplify $\varphi_p'(\zeta_p)$.)

Tool 1. [Bak22, Lemma 2.3] *Let $\beta_1, \beta_2, \ldots, \beta_n$ be n algebraic integers that generate a subgroup of index m of $\mathcal{O}_K$. Then*

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) = m^2 \Delta_K.$$

In particular, if $\Delta(\beta_1, \beta_2, \ldots, \beta_n)$ is squarefree, then $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is an integral basis.

This result can be derived from the geometric interpretation of the discriminant as in Exercise 9. We will now use this tool to give some explicit upper bounds on the index in various examples.

Example 11. Let $f(x) = x^2 - d$. Then

$$\Delta(1, \sqrt{d}) = \det \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}^2 = 4d.$$

Since m^2 divides $\Delta(1, \sqrt{d}) = 4d$ and d is squarefree, this tells us m is either 1 or 2. We already saw that when d is $\equiv 1 \mod 4$, the element $(1 + \sqrt{d})/2$ is an algebraic integer and we have the inclusions

$$\mathbb{Z}[\sqrt{d}] \subsetneq \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subset \mathcal{O}_K.$$

Since the only subgroups of the quotient group $\mathcal{O}_K/\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}/2\mathbb{Z}$ are the trivial group and the whole group, this tells us $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathcal{O}_K$ when $d \equiv 1 \mod 4$.

Example 12. Let $f(x) = x^3 - 2x + 3$. Using exercise 10, we compute the discriminant of the power basis corresponding to α to be $-4(-2)^3 - 27 \cdot 3^2 = -211$. Since -211 is prime, we conclude that $\mathbb{Z}[\alpha] = \mathcal{O}_K$.

Example 13. Let $f(x) = x^3 - 2$. Using exercise 10, we compute the discriminant of the power basis corresponding to α to be $-4 \cdot 0^3 - 27 \cdot (-2)^2 = -108 = -2^2 3^3$. Since m^2 divides -108, we conclude that the index m of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ is one of $1, 2, 3, 6$.

Example 14. Let $f(x) = x^{p-1} + x^{p-2} + \ldots + 1$ be the p-th cyclotomic polynomial for a prime p. Using exercice 10, the discriminant of the power basis corresponding to α is p^{p-1}, and we conclude that the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ is one of $1, p, \ldots, p^{(p-1)/2}$.

1.2 Ruling out prime divisors of the index

Tool 2. [Bak22, Proposition 2.9] *If f is Eisenstein at p (i.e. if $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$ then p divides a_i for every i, but $p^2 \nmid a_n$), then p does not divide the index $[\mathcal{O}_K : Z[\alpha]]$.*

Example 15 (Revisiting Example 13). Since the polynomial $f(x) = x^3 - 2$ is Eisenstein at 2, this tells us that 2 does not divide the index m of $\mathbb{Z}[\sqrt[3]{2}]$ in $\mathcal{O}_K$. Since we already showed that the only possibilities for m are $1, 2, 3, 6$ in Example 13, the only remaining possibilities are $m = 1$ and $m = 3$. In fact, by instead working with the algebraic integer $\beta := \alpha - 2 = \sqrt[3]{2} - 2$, which generates the same subring as $\sqrt[3]{2}$, i.e. $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, we can also rule out $m = 3$. Indeed, the element β has minimal polynomial $(x + 2)^3 - 2 = x^3 + 6x^2 + 12x + 6$, which is Eisenstein at *both* 2 and 3, so neither 2 nor 3 can divide the index of $\mathbb{Z}[\beta]$ in $\mathcal{O}_K$.

Example 16 (Revisiting Example 14). Let $f(x) = x^{p-1} + x^{p-2} + \ldots + 1$ with root α. The element $\beta = \alpha - 1$ generates the same subring as α, but has minimal polynomial that is Eisenstein at p. So p cannot divide the index of $\mathbb{Z}[\beta]$ in $\mathcal{O}_K$. Since $\mathbb{Z}[\beta] = \mathbb{Z}[\alpha]$ and we already showed in Example 14 that the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ is a power of p, it follows that $m = 1$, i.e. that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

1.3 Enlarging the subgroup

Tool 3. [Bak22, Lemma 2.5(b)] *If $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a collection of algebraic integers generating an index m subgroup of $\mathcal{O}_K$ and $m \neq 1$, then $\mathcal{O}_K$ contains an element of the form*

$$m_1 \frac{\alpha_1}{m} + \cdots + m_n \frac{\alpha_n}{n},$$

with $0 \leq m_i \leq m-1$ and not all m_i equal to 0.

This tells us that we can iteratively enlarge our finite index subgroup to be the full ring of integers by testing if one of the $m^n - 1$ algebraic numbers in the set above is an algebraic integer.

Example 17. [Revisiting Example 11] Let d be a squarefree integer. We showed in Example 11 that the index of $\mathbb{Z}[\sqrt{d}]$ in $\mathcal{O}_K$ for the number field $K = \mathbb{Q}(\sqrt{d})$ is either 1 or 2. If the index is 2, the fact above tells us that one of the three numbers in the set

$$\{1/2, \sqrt{d}/2, (1+\sqrt{d})/2\}$$

must be an algebraic integer. We already showed in Example 11 that if $d \equiv 1 \mod 4$, then $\mathbb{Z}[\sqrt{d}]$ has index 2 in $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{d})/2]$. If d is 2 or 3 modulo 4, then none of these three numbers is an algebraic integer, as is evident from their minimal polynomials $2x-1, 4x^2-d$ and 1, and it follows that $\mathbb{Z}[\sqrt{d}] = \mathcal{O}_K$.

1.4 Algorithm for computing $\mathcal{O}_K$

An algorithm for computing $\mathcal{O}_K$ for an arbitrary number field K now goes as follows. Choose a primitive element α for K. Multiply α by a suitable nonzero integer m to make a new primitive element that is also an algebraic integer (Exercise 2). The powers of $m\alpha$ now generate a finite index subgroup of $\mathcal{O}_K$. Compute $\Delta(m\alpha)$ to get a bound on the index $[\mathcal{O}_K : \mathbb{Z}[m\alpha]]$ using Tool 1 (narrow down the possibilities for the index further using 2 if possible). Enlarge your finite index subgroup to all of $\mathcal{O}_K$ by iteratively using Tool 3.

Suggested exercises 18. Let $K = \mathbb{Q}(\sqrt{7}, \sqrt{-2})$. Enlarge the finite index subgroup of $\mathcal{O}_K$ spanned by $1, \sqrt{7}, \sqrt{-2}, \sqrt{-14}$ to a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

Number field	**Restrictions**	**Ring of integers**
$\mathbb{Q}$		$\mathbb{Z}$
$\mathbb{Q}(\sqrt{d})$	$d \cong 2, 3 \mod 4$ squarefree	$\mathbb{Z}[\sqrt{d}]$
$\mathbb{Q}(\sqrt{d})$	$d \cong 1 \mod 4$ squarefree	$\mathbb{Z}[(1+\sqrt{d})/2]$
$\mathbb{Q}(\sqrt[3]{2})$		$\mathbb{Z}[\sqrt[3]{2}]$
$\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$	$d_1, d_2 \cong 1 \mod 3$, distinct, squarefree	not monogenic, see [Wil70]
$\mathbb{Q}(\zeta_p)$ p-th cyclotomic field	p prime ≥ 3	$\mathbb{Z}[\zeta_p]$

2 Unique factorization in ring of integers, or lack thereof

The key property about $\mathbb{Z}$ that was used to justify the existence of a representative of $[x_0 : x_1 : \ldots : x_n]$ with $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$ was the unique factorization of the integers – this was crucial for our definition of heights of points in $\mathbb{P}^n(\mathbb{Q})$. Unfortunately, unique factorization can fail for general rings of algebraic integers, as the following example illustrates. For example, when $K = \mathbb{Q}(\sqrt{-5})$, by Example 17 we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. There are two distinct factorizations of the element 6 into a product of irreducible elements:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Suggested exercises 19. Verify that $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are four mutually non-associate irreducible elements in the ring $\mathbb{Z}[\sqrt{-5}]$ that are not prime.

Knowing unique factorization in number rings can have interesting Diophantine consequences. The first section of [Bak22] shows how unique factorization in the ring of Gaussian integers $\mathbb{Z}[i]$ can be used to prove that the only integral point (i.e. a solution in $\mathbb{Z}^2$) on the elliptic curve $y^2 = x^3 - 1$ is $(1, 0)$ – we strongly encourage the interested reader to read this fun argument! Trying to adapt a similar argument to prove Fermat's last theorem was one of the main reasons that lead Kummer to study unique factorization in more general number rings. For the application to Fermat's last theorem, he needed to know if the ring of integers of the cyclotomic field $\mathbb{Z}[\zeta_p]$ is a unique factorization domain. He realized that it was hardly every true. (Sadly $\mathbb{Z}[\zeta_p]$ is a UFD only for $p \leq 19$! This was proved after Kummer's time.)

However, Kummer showed that unique factorization can be salvaged, and developed several ideas in modern Algebraic number theory to establish many new cases of Fermat's last theorem. He showed that although every *element* does not factor uniquely into a product of *irreducible elements* (up to units), every *ideal* does factor uniquely into a product of *prime ideals*. In fact, the word *ideal number* was coined by Kummer as a substitute for numbers in an ideal world, for example in rings of integers where unique factorization failed. The concrete set theoretic definition of ideals that we learn today was developed by Dedekind. Rings having unique factorization of ideals are nowadays called Dedekind domains.

Theorem 20. [Bak22, Chapter 1, Theorem 1.27] *(Kummer) Every ideal of $\mathcal{O}_K$ factors uniquely into a product of powers of prime ideals.*

For example, in the example $\mathbb{Z}[\sqrt{-5}]$ above, we have the four prime ideals

$$\mathfrak{p}_1 = (2, 1 + \sqrt{-5}), \qquad \mathfrak{p}_2 = (2, 1 - \sqrt{-5}),$$
$$\mathfrak{p}_3 = (3, 1 + \sqrt{-5}), \qquad \mathfrak{p}_4 = (3, 1 + \sqrt{-5}),$$

and the factorizations

$$(2) = \mathfrak{p}_1\mathfrak{p}_2,$$
$$(3) = \mathfrak{p}_3\mathfrak{p}_4,$$
$$(1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3,$$
$$(1 - \sqrt{-5}) = \mathfrak{p}_4\mathfrak{p}_4, \text{and}$$
$$(6) = (2) \cdot (3) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_3\mathfrak{p}_4) = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Suggested exercises 21. Verify that the ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ as above are prime (and even maximal) ideals.

It turns out that Fact 20 is sufficient for the purposes of defining a height function on $\mathbb{P}^n(K)$ for K a number field. Our next goal is to understand how to explicitly write down prime ideals of $\mathcal{O}_K$, and then how to use these prime ideals to build absolute values on number fields. A classification of absolute values on K is one of the key inputs for defining heights on $\mathbb{P}^n(K)$.

Suggested exercises 22. Consider the affine elliptic curve with equation $y^2 - x^3 + x \in \mathbb{C}[x, y]$ and its associated affine coordinate ring $S := \mathbb{C}[x, y]/(y^2 - x^3 + x)$.

(a) Let a be a complex number. Prove that if $a \notin \{-1, 0, 1\}$, then $S/(x - a)S$ has exactly two prime ideals, whose lifts $\mathfrak{p}_1, \mathfrak{p}_2$ to S satisfy $(x - a)S = \mathfrak{p}_1\mathfrak{p}_2$ (the "completely split" case), and that if $a \in \{-1, 0, 1\}$, then $S/(x - a)S$ has a unique prime ideal $\mathfrak{p}$ and $(x - a)S = \mathfrak{p}^2$ (the "ramified" case).

(b) Show that every nonzero prime ideal of S is of the form $(x - a, y - b)$ for some complex numbers a and b. (Hint: Show that the intersection of a nonzero prime ideal of S with $\mathbb{C}[x]$ is a *nonzero prime* ideal of $\mathbb{C}[x]$, and hence of the form $(x - a)$ for some complex number a.)

References

[Bak22] Matt Baker, *Algebraic Number Theory Course Notes* (2022). ↑1, 2, 3, 4, 5, 6, 7

[Wil70] Kenneth S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull. **13** (1970), 519–526, DOI 10.4153/CMB-1970-094-8. MR279069 ↑6