13. Algebraic number theory

Definition 13.1. *Let $\alpha \in \mathbb{C}$ be a complex number.*

*We say that α is **algebraic** if there is a polynomial*

$$p(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$$

such that $p(\alpha) = 0$.

Example 13.2. *Any rational number is algebraic.*

Indeed, $p(x) = x - \alpha \in \mathbb{Q}[x]$ and of course $p(\alpha) = 0$.

Example 13.3. *$\sqrt{2}$ is algebraic.*

Indeed $p(x) = x^2 - 2 \in \mathbb{Q}[x]$ and $p(\sqrt{2}) = 0$. More generally, $\sqrt{d}$ is algebraic, as it is one of the zeroes of $x^2 - d$.

Example 13.4. *i is algebraic.*

Indeed i is a zero of $x^2+1 \in \mathbb{Q}[x]$. Perhaps not surprisingly the more complicated $p(x)$, the more complicated α. However if α is a zero of $p(x)$ then α is a zero of $p(x)q(x)$ for any polynomial $q(x)$.

Definition-Lemma 13.5. *Let $\alpha \in \mathbb{C}$ be algebraic.*

*The **minimal polynomial** of α, denoted $m_\alpha(x) \in \mathbb{Q}[x]$, is the smallest degree polynomial such that α is a zero of $m_\alpha(x)$.*

The minimal polynomial is irreducible and it divides any other polynomial for which α is a zero.

*The **degree** of α is the degree of $m_\alpha(x)$.*

Proof. If $p(\alpha) = 0$ and $p(x) = q(x)r(x)$ then either $q(\alpha) = 0$ or $r(\alpha) = 0$.

It is therefore clear that the minimal polynomial is irreducible. Suppose that $p(\alpha) = 0$. We may write

$$p(x) = q(x)m_\alpha(x) + r(x),$$

where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $m_\alpha(x)$.

We have

$$\begin{aligned} 0 &= p(\alpha) \\ &= q(\alpha)m_\alpha(\alpha) + r(\alpha) \\ &= r(\alpha). \end{aligned}$$

As $r(\alpha) = 0$ and $m_\alpha(x)$ is the minimal polynomial, it follows that $r(x) = 0$, so that $m_\alpha(x)$ divides $p(x)$. $\square$

Rational numbers have degree one and $\sqrt{2}$ has degree two.

It is not hard to see that the collection of all polynomials in α is a subring of the field of all complex numbers. It is denoted $\mathbb{Q}[\alpha]$. For example $\mathbb{Z}[i]$ the Gausian integers (note that $i^2 = -1$) and the ring $\mathbb{Z}[\sqrt{d}]$ behind Pell's equation

Theorem 13.6. *If α is an algebraic number then*

$$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$$

is a field and not just a ring.

It is generated as a vector space over $\mathbb{Q}$ by the powers of α up to $n-1$; in particular it is finite dimensional over $\mathbb{Q}$.

Further,

$$\mathbb{Q}[\alpha] = \frac{\mathbb{Q}[x]}{\langle m_\alpha(x) \rangle}.$$

Proof. Define a ring homomorphism

$$\mathbb{Q}[x] \longrightarrow \mathbb{Q}[\alpha] \qquad \text{by the rule} \qquad x \longrightarrow \alpha.$$

This map is clearly surjective. The kernel is the set of all polynomials which have α as a zero. We have already seen that this is the set of all multiples of $m_\alpha(x)$. This gives the isomorphism.

To show that

$$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$$

we have to show that the LHS is a field, that is, we have to show that every non-zero element of $\mathbb{Q}[\alpha]$ has an inverse. We are given $f(x) \in \mathbb{Q}[x]$ and we want to construct the inverse modulo $m_\alpha(x)$. $m_\alpha(x)$ is irreducible and does not divide $f(x)$. It follows that we may find $a(x)$ and $b(x)$ such that

$$1 = a(x)f(x) + b(x)m_\alpha(x).$$

But then $a(x)$ is the inverse of $f(x)$, modulo $m_\alpha(x)$.

We check that 1, α, α^2, $\dots$, α^{n-1} are a basis for $\mathbb{Q}[\alpha]$. If they were dependent we could find $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ such that

$$\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \cdots + \lambda^{n-1}\alpha^{n-1} = 0.$$

If we put

$$f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \cdots + \lambda^{n-1}x^{n-1},$$

then $f(x)$ is a polynomial with rational coefficients. As $f(\alpha) = 0$ and $f(x)$ has smaller degree than $m_\alpha(x)$ it follows that $f(x) = 0$. But then $\lambda_i = 0$ for $0 \leq i \leq n-1$. It follows that 1, α, α^2, $\dots$, α^{n-1} are independent.

We now check they span. It is clear that all of the powers span and so we just need to check that we can get every power of α. So we just need to check that if $m \geq n$ then we can express α^m in terms of lower powers of α. But this is clear. As

$$m_\alpha(\alpha) = 0,$$

α^n is a linear combination of lower powers of α. Multiplying through by α^{m-n}, we express α^m in terms of lower powers. $\square$

It is also possible to define the norm of α:

Definition 13.7. *If $\alpha \in \mathbb{C}$ is algebraic then the* ***norm*** *of α, denoted $N(\alpha)$, is $(-1)^n a_0$, where a_0 is the constant term of $m_\alpha(x)$.*

Note that the norm of α is the product of the roots of $m_\alpha(x)$. For example, $\sqrt[3]{2}$ is algebraic and its norm is 2, as $m_{\sqrt[3]{2}}(x) = x^3 - 2$.

Perhaps the most interesting issue is to decide what should be the integers in the field $\mathbb{Q}(\alpha)$. It cannot be $\mathbb{Q}[\alpha]$, since this is the whole field.

Definition 13.8. *$\alpha \in \mathbb{C}$ is called an* ***algebraic integer*** *if α is algebraic and $m_\alpha(x) \in \mathbb{Z}[x]$.*

It is a standard result of abstract algebra that the set of all algebraic integers is a ring, so that the sum and product of two algebraic integers is an algebraic integer. So if α is an algebraic integer then the ring generated by $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{Q}(\alpha)$ consisting of algebraic integers.

One subtle issue is that there might be more algebraic integers. For example

$$\sqrt{2} \notin \mathbb{Z}[2\sqrt{2}] \qquad \text{and yet} \qquad \sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

A much more interesting example is given by

$$\beta = \frac{1}{2}(1 + \sqrt{5}).$$

Define

$$\bar{\beta} = \frac{1}{2}(1 - \sqrt{5}).$$

Then

$$\beta + \bar{\beta} = 1 \qquad \text{and} \qquad \beta\bar{\beta} = -1.$$

Thus β is a root of

$$x^2 - x - 1 = 0,$$

so that β is an algebraic integer.

Definition-Lemma 13.9. *A field $\mathbb{Q} \subset F \subset \mathbb{R}$ such that $F/\mathbb{Q}$ is a finite dimensional vector space is called a* ***number field****. The set of all algebraic integers in F, denoted $\mathcal{O}_F$, is called a* ***number ring****.*

A ***unit*** *ϵ is an invertible element of $\mathcal{O}_F$. $\epsilon \in \mathcal{O}_F$ is a unit if and only if $N(\epsilon) = \pm 1$.*

Proof. If
$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$
is the minimal polynomial of ϵ then
$$\epsilon^n + a_{n-1}\epsilon^{n-1} + a_{n-2}\epsilon^{n-2} + \cdots + a_1\epsilon + a_0 = 0.$$
Dividing through by ϵ^n gives
$$1 + a_{n-1}(\epsilon)^{-1} + a_{n-2}(\epsilon)^{-2} + \cdots + a_1\epsilon^{1-n} + a_0(\epsilon)^{-n} = 0.$$
Thus
$$x^n + \frac{a_1}{a_0}x^{n-1} + \frac{a_2}{a_0}x^{n-2} + \cdots + \frac{a_{n-1}}{a_0}x + \frac{a_n}{a_0}.$$
is a monic polynomial and $1/\epsilon$ is a root. It is not hard to see that this monic polynomial is irreducible and so it has integer coefficients if and only if $a_0 = \pm 1$. But $N(\epsilon) = \pm a_0$. $\square$

As with any integral domain, one can define divides, associates, irreducible and prime. If α and $\beta \in \mathcal{O}_F$ then α divides β if we can find $\gamma \in \mathcal{O}_F$ suhc that $\beta = \alpha\gamma$. α and β are associates if α divides β and β divides α. This is the same as to say $\alpha = \beta\epsilon$, where ϵ is a unit.

Usually irreducible is defined to mean that one cannot factor anymore and prime is defined to mean that if one divides a product then one divides one of the factors. Unfortunately the definition of prime in a number ring is the same as irreducible.