Algebraic Number Theory

Term 2, 2018–19

Martin Orr

1. Introduction

Gaussian integers.

The simplest example of what we will study in Algebraic Number Theory is the Gaussian integers

$$\{a + bi : a, b \in \mathbb{Z}\}.$$

If you did Introduction to Number Theory, you will have seen these before, but whether you have or not we will see them in this course as a special case of a much broader theory.

The key points about the Gaussian integers:

(1) We can describe the irreducible Gaussian integers in terms of the ordinary prime numbers (depending on whether a prime is 1 or 3 mod 4).
(2) Every Gaussian integer can be uniquely factorised as a product of irreducible Gaussian integers.

Gaussian integers are an example of algebraic integers i.e. numbers which are a root of a monic polynomial with integer coefficients. Algebraic Number Theory is about doing number theory with other algebraic integers, for example describing the primes in a ring of algebraic integers or deciding whether a ring of algebraic integers has unique factorisation.

Usually, a ring of algebraic integers does not have unique factorisation. We will define factorisation of ideals, instead of elements of the ring, and see that this restores the uniqueness of prime factorisations. We will also define the "class group" of an algebraic number ring, which measures how far it is away from having unique factorisation of elements.

Practical information about the course.

The course involves a lot of down-to-earth calculation with examples e.g. determining how a prime factorises in a number field or computing the class group of a number field. There is also a good deal of theory underpinning these calculations. Lectures will focus on the theory; example sheets and support classes on the examples.

Assignments – four pieces, best 3 of 4 will count (15% of module mark)
Deadlines: Friday 2pm in weeks 3, 6, 8, 10
Example sheets and lecture capture will be available on Moodle.
My email address: `martin.orr@warwick.ac.uk`
Office hours: Fri 2-3, Zeeman C2.11

Course outline.

(1) Number fields and embeddings
(2) Rings of integers
(3) Ideals and factorisation
(4) Class group
(5) Dirichlet's unit theorem

Related courses.

MA249 Algebra 2 – prerequisite. Rings, fields, ideals and factorisation of polynomials will be used throughout this course. We will also need quotient rings and the First Isomorphism Theorem for rings. Revise this!

MA257 Introduction to Number Theory – not strictly a prerequisite, but it will provide very helpful background.

MA3D5 Galois Theory – There is some overlap in the first 1–2 weeks, with various definitions and lemmas related to field extensions. We shall go through these again in this course.

Field extensions.

Our main object of study will be number fields. A number field is defined as a finite extension of the field $\mathbb{Q}$. Let's unpack this definition.

Definition. Let K and L be fields. If K is a subfield of L, we say that L/K is a **field extension** (often, we will just call it an **extension**).

e.g. $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}(i)$ but not $\mathbb{R}/\mathbb{Q}(i)$
where $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

Definition. Let L/K be a field extension and $\alpha \in L$. We say that α is **algebraic over** K if there exists a non-zero polynomial $f \in K[X]$ such that $f(\alpha) = 0$.

e.g. $i \in \mathbb{C}$, $\sqrt[4]{7} \in \mathbb{R}$ are algebraic over $\mathbb{Q}$
πi is algebraic over $\mathbb{R}$ but not algebraic over $\mathbb{Q}$

Lemma 1. Let α be algebraic over K.

(i) There exists a unique monic polynomial $\mu_{K,\alpha}(X) \in K[X]$ of smallest degree such that $\mu_{K,\alpha}(\alpha) = 0$. (**monic** means that the leading coefficient is 1 – this forces the polynomial to be non-zero.)
(ii) If $f \in K[X]$ satisfies $f(\alpha) = 0$, then $\mu_{K,\alpha}$ divides f.
(iii) $\mu_{K,\alpha}$ is irreducible.
(iv) If $f \in K[X]$ is monic and irreducible and $f(\alpha) = 0$, then $f = \mu_{K,\alpha}$.

Proof.

(i)+(ii) Let $I = \{f \in K[X] : f(\alpha) = 0\}$. One can check that this is an ideal in $K[X]$.

Recall from Algebra 2 that $K[X]$ is a PID (principal ideal domain) so $I = (\mu_{K,\alpha})$ for some $\mu_{K,\alpha} \in K[X]$.

Since α is algebraic over K, $I \neq \{0\}$ so $\mu_{K,\alpha} \neq 0$. Therefore we can multiply $\mu_{K,\alpha}$ by a scalar to ensure that it is monic.

Clearly $\mu_{K,\alpha}$ has the smallest degree of all polynomials in I, and it satisfies (ii) by the definition of a principal ideal.

(ii) implies that there is no other monic polynomial in I with the same degree as $\mu_{K,\alpha}$, i.e. it is unique.

(iii) Suppose $\mu_{K,\alpha} = fg$. Then $f(\alpha)g(\alpha) = 0$. Since L is a field, either $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss of generality, $f(\alpha) = 0$. By (ii), $\mu_{K,\alpha}$ divides f so g must be a constant. Thus $\mu_{K,\alpha}$ is irreducible.

(iv) Consequence of (ii). □

Definition. The polynomial $\mu_{K,\alpha}$ from Lemma 1 is called the **minimal polynomial** of α over K.

We will write μ_α instead of $\mu_{K,\alpha}$ if the base field K is clear from the context.

But! K matters for determining the minimal polynomial! e.g. $\alpha = i + \sqrt{2} \in \mathbb{C}$.

- Over $K = \mathbb{C}$: the minimal polynomial is $\mu_{\mathbb{C},\alpha}(X) = X - \alpha$.
- Over $K = \mathbb{R}$: $\alpha \notin \mathbb{R}$, so the minimal polynomial has degree > 1. A calculation shows that $\mu_{\mathbb{R},\alpha}(X) = X^2 - 2\sqrt{2}X + 3$.

Question. What is the minimal polynomial of $\alpha = i + \sqrt{2}$ over $\mathbb{Q}$?

2. Algebraic extensions

Example from last time.

- Over $K = \mathbb{R}$: We have
$$(\alpha - \sqrt{2})^2 = -1 \quad \text{so} \quad \alpha^2 - 2\sqrt{2}\alpha + 3 = 0.$$
$X^2 - 2\sqrt{2}X + 3 \in \mathbb{R}[X]$ is irreducible over $\mathbb{R}$ because it is a quadratic with no real roots. So $\mu_{\mathbb{R},\alpha}(X) = X^2 - 2\sqrt{2}X + 3$.
- Over $K = \mathbb{Q}$: α is algebraic over $\mathbb{Q}$ because
$$(\alpha^2 + 3)^2 = (2\sqrt{2}\alpha)^2 = 8\alpha^2 \quad \text{so} \quad \alpha^4 - 2\alpha^2 + 9 = 0.$$
One can check that $X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$, so this is $\mu_{\mathbb{Q},\alpha}$. We will see a quicker proof later (avoiding checking irreducibility by hand).

Definition. Let $\alpha \in L$ be algebraic over K. The **degree of α over K** is the degree of the polynomial $\mu_{K,\alpha}$.

e.g. $i + \sqrt{2}$ has degree 1 over $\mathbb{C}$, 2 over $\mathbb{R}$, 4 over $\mathbb{Q}$.

Field generation.

Definition. Let L/K be a field extension and let S be a subset of L. The **extension of K generated by** S is the smallest subfield of L containing both K and S.

This means: the intersection of all subfields of L which contain both K and S. Check that this intersection is a field!

Written $K(S)$. If S is finite set $\{\alpha_1, \ldots, \alpha_n\}$, we write $K(\alpha_1, \ldots, \alpha_n)$ as an abbreviation for $K(\{\alpha_1, \ldots, \alpha_n\})$.

e.g. $\mathbb{C} = \mathbb{R}(i)$

If d is a non-square rational number, then
$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$
This is a field because
$$(a + b\sqrt{d})(c + e\sqrt{d}) = (ac + bed) + (ae + bc)\sqrt{d}$$
and
$$(a + b\sqrt{d})^{-1} = (a - b\sqrt{d})/(a^2 - db^2)$$
(the denominator is non-zero because d is not the square of a rational number).

But! $\mathbb{Q}(\sqrt[3]{d}) \neq \{a + b\sqrt[3]{d} : a, b \in \mathbb{Q}\}$ because this is not closed under multiplication. We will soon see how to write down a basis for $\mathbb{Q}(\sqrt[3]{d})$.

In general, $K(S)$ is the set of everything of the form $f(\alpha_1, \ldots, \alpha_r)/g(\beta_1, \ldots, \beta_s)$ where f, g are polynomials (in any number of variables) with coefficients in K, $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in S$ and $g(\beta_1, \ldots, \beta_s) \neq 0$.

Algebraic and finite extensions.

Definition. An extension L/K is **algebraic** if every $\alpha \in L$ is algebraic over K.

e.g. $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is algebraic since $a + b\sqrt{d}$ is a root of $(X-a)^2 - b^2 d \in \mathbb{Q}[X]$.
$\mathbb{R}/\mathbb{Q}$ is not algebraic.

Definition. If L/K is a field extension, then L is a K-vector space. The **degree** of L/K, written $[L:K]$, is the dimension of L as a K-vector space.

Definition. L/K is a **finite extension** if its degree is finite.

e.g. $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}] = 2, \quad [\mathbb{C}:\mathbb{R}] = 2.$
$\mathbb{Q}(\pi)/\mathbb{Q}$ has infinite degree, even though it is generated by the finite set $\{\pi\}$, because $1, \pi, \pi^2, \ldots$ are $\mathbb{Q}$-linearly independent.

Lemma 2. If L/K is a finite extension, then it is an algebraic extension.

Proof. Let $m = [L:K] < \infty$. Let $\alpha \in L$. Then $1, \alpha, \ldots, \alpha^m$ are $m+1$ elements in a K-vector space of dimension m, so they are K-linearly dependent. In other words, there exist $\lambda_0, \ldots, \lambda_m \in K$, not all zero, such that

$$\lambda_0 + \lambda_1 \alpha + \cdots + \lambda_m \alpha^m = 0.$$

Thus α is the root of the polynomial $\lambda_0 + \lambda_1 X + \cdots + \lambda_m X^m \in K[X]$, so it is algebraic over K. □

The converse is false: the field of all algebraic numbers in $\mathbb{C}$ is an algebraic extension of $\mathbb{Q}$, but not a finite extension of $\mathbb{Q}$ (though we have not proved that this is a field yet).

Tower law.

Often we build field extensions by stacking one on top of another. The following theorem tells us how to calculate the degree of such an extension.

Theorem (Tower Law)**.** Let M/L and L/K be two finite field extensions. Then M/K is also a finite extension, and

$$[M:K] = [M:L][L:K].$$

Proof. Let $r = [L:K]$ and $s = [M:L]$. Let $\{\ell_1, \ldots, \ell_r\}$ be a K-basis for L and let $\{m_1, \ldots, m_s\}$ be an L-basis for M.

One can check that $\{l_i m_j : 1 \le i \le r, 1 \le j \le s\}$ is a K-basis for M. □

e.g. $M = \mathbb{Q}(\alpha)$ where $\alpha = i + \sqrt{2}, \quad L = \mathbb{Q}(\sqrt{2}), \quad K = \mathbb{Q}$
We saw that

$$\sqrt{2} = \frac{\alpha^2 + 3}{2\alpha}$$

so $L \subseteq M$.

Now $M = L(\alpha)$. To prove this: certainly L and α are both contained in M, so $L(\alpha) \subseteq M$. Furthermore, $L(\alpha)$ is a field which contains $\mathbb{Q}$ and α, so the definition of $\mathbb{Q}(\alpha)$ tells us that $L(\alpha) \supseteq \mathbb{Q}(\alpha) = M$. Thus $L(\alpha) = M$.

In fact, $L(\alpha) = L(i)$ because $i = \alpha - \sqrt{2}$ and $\sqrt{2} \in L$ (this is slightly simpler than the argument I gave in the lecture, using the quadratic formula). Note that $i \notin L$ because $L \subseteq \mathbb{R}$. We can show that $[L(i) : L] = 2$ for the same reason as $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$. Thus we get $[M : L] = 2$.

We also have $[L : K] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

So the Tower Law tells us that $[M : K] = 2 \times 2 = 4$.

The fact that $\mu_{\mathbb{Q},\alpha}$ has degree 4 is not a coincidence! We will see how to relate these facts (and thereby prove that $\mu_{\mathbb{Q},\alpha}$ has degree 4) in the next lecture.

3. Simple extensions and number fields

Simple extensions.

Definition. An extension L/K is **simple** if $L = K(\alpha)$ for a *single* element $\alpha \in L$.

Note that a simple extension need not be finite, e.g. $\mathbb{Q}(\pi)/\mathbb{Q}$. But if it is algebraic, then it is finite and we can describe the extension in terms of the minimal polynomial of α:

Theorem 3. Let α be algebraic over K, with minimal polynomial $\mu_\alpha \in K[X]$. Let $n = \deg(\mu_\alpha)$. Then:

(1) $K(\alpha)$ is isomorphic as a ring to $K[X]/(\mu_\alpha)$. More precisely, the following is a well defined isomorphism $K[X]/(\mu_\alpha) \to K(\alpha)$:
$$f(X) + (\mu_\alpha) \mapsto f(\alpha).$$
(2) $K(\alpha)$ has K-basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$.
$[K(\alpha) : K] = n$.

Proof. (1) Define $\phi\colon K[X] \to K(\alpha)$ by $\phi(f(X)) = f(\alpha)$.
One can check that this is a ring homomorphism.
From the proof of Lemma 1, we see that
$$\ker(\phi) = \{f \in K[X] : f(\alpha) = 0\} = (\mu_\alpha).$$
Hence by the first isomorphism theorem, ϕ induces an isomorphism $K[X]/(\mu_\alpha) \to \mathrm{im}(\phi)$. We just have to check that $\mathrm{im}(\phi) = K(\alpha)$.

Step 1. First we prove that $1, \alpha, \ldots, \alpha^{n-1}$ span $\mathrm{im}(\phi)$ as a K-vector space.
For any $\beta \in \mathrm{im}(\phi)$, we have $\beta = \phi(f)$ for some $f \in K[X]$. By the division algorithm for polynomials, we can write
$$f = q\mu_\alpha + r$$
where $q, r \in K[X]$ and $\deg(r) < \det(\mu_\alpha)$. Then
$$\beta = f(\alpha) = r(\alpha) = c_0 + c_1\alpha + \cdots + c_s\alpha^s$$
where $c_0, c_1, \ldots, c_s \in K$ and $s = \deg(r) < n$. Thus β is in the span of $1, \alpha, \ldots, \alpha^{n-1}$.

Step 2. We show that $\mathrm{im}(\phi)$ is a field. This is just one of many possible proofs.
We know that $\mathrm{im}(\phi)$ is a ring, so we just have to show that every $x \in \mathrm{im}(\phi) \setminus \{0\}$ has a multiplicative inverse in $\mathrm{im}(\phi)$.
Given $x \in \mathrm{im}(\phi) \setminus \{0\}$, define a K-linear map $m_x\colon \mathrm{im}(\phi) \to \mathrm{im}(\phi)$ by
$$m_x(y) = xy.$$
This is injective because $\mathrm{im}(\phi) \subseteq K(\alpha)$ which is a field.
Therefore by the rank-nullity theorem, m_x is surjective (this uses the fact that $\mathrm{im}(\phi)$, is finite-dimensional as a K-vector space, which follows from Step 1). Therefore there exists $y \in \mathrm{im}(\phi)$ such that $m_x(y) = 1$ i.e. $y = 1/x$.
Thus $\mathrm{im}(\phi)$ is a field.

Conclusion of (1). $\mathrm{im}(\phi)$ contains K and $\alpha = \phi(X)$, so by the definition of $K(\alpha)$, $K(\alpha) \subseteq \mathrm{im}(\phi)$. But also $\mathrm{im}(\phi) \subseteq K(\alpha)$. Thus $\mathrm{im}(\phi) = K(\alpha)$.

(2) We saw in Step 1 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ spans $\mathrm{im}(\phi) = K(\alpha)$ as a K-vector space. We just have to show that $1, \alpha, \ldots, \alpha^{n-1}$ are K-linearly independ

Suppose we have $b_0, \ldots, b_{n-1} \in K$ such that

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0.$$

Then $g(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$ is a polynomial in $K[X]$ such that $g(\alpha) = 0$ and $\deg(g) \leq n-1 < \deg(\mu_\alpha)$ so the definition of minimal polynomial forces $g \equiv 0$ i.e. $b_0 = b_1 = \cdots = b_{n-1}$. □

e.g. We can immediately read off that $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{d})$ (as we saw already).

If $d \in \mathbb{Q}$ is not a cube, then $X^3 - d$ is irreducible so it is the minimal polynomial of $\sqrt[3]{d}$. So $[\mathbb{Q}(\sqrt[3]{d}) : \mathbb{Q}] = 3$ and

$$\mathbb{Q}(\sqrt[3]{d}) = \{a + b\sqrt[3]{d} + c\Big(\sqrt[3]{d}\Big)^2 : a, b, c \in \mathbb{Q}\}.$$

Returning to the example from the previous lecture: $\alpha = i + \sqrt{2}$, $M = \mathbb{Q}(\alpha)$. Using the Tower Law, we proved that $[M : \mathbb{Q}] = 4$. Therefore Theorem 3 tells us that $\deg(\mu_{\mathbb{Q},\alpha}) = 4$.

We also saw that α is a root of the polynomial $g(X) = X^4 - 2X^2 + 9$. Hence $\mu_{\mathbb{Q},\alpha} = g$ and g is irreducible over $\mathbb{Q}$ (by Lemma 1).

Theorem 3 tells us that a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$ is given by

$$\{1, \alpha, \alpha^2, \alpha^3\} = \{1, \sqrt{2} + i, 1 + 2\sqrt{2}i, -\sqrt{2} + 5i\}.$$

We can get a different $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$ from the proof of the Tower Law. Indeed, $\mathbb{Q}(\sqrt{2})$ has a $\mathbb{Q}$-basis $\{1, \sqrt{2}\}$ while $\mathbb{Q}(\alpha)$ has a $\mathbb{Q}(\sqrt{2})$-basis $\{1, i\}$ (follows from the argument with the quadratic formula). Thus the proof of the Tower Law gives us the following $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$:

$$\{1, \sqrt{2}, i, i\sqrt{2}\}.$$

Number fields.

Definition. A **number field** is a finite extension of $\mathbb{Q}$.

Lemma 4. Let K be a number field and let L/K be a finite extension. Then L is also a number field.

Proof. This follows from the Tower Law. □

Definition. An **algebraic number** is an element of $\mathbb{C}$ which is algebraic over $\mathbb{Q}$.

Lemma 5. If $\alpha_1, \ldots, \alpha_n$ are algebraic numbers, then $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is a number field.

Proof. Let $K_i = \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ for $1 \leq i \leq n$. We prove that K_i is a number field by induction on i.

The base case is that $K_0 = \mathbb{Q}$ is a number field.

For $i \geq 1$: Since α_i is an algebraic number, it has a minimal polynomial $\mu_{\mathbb{Q},\alpha_i}$. We have $\mu_{\mathbb{Q},\alpha_i}(X) \in \mathbb{Q}[X] \subseteq K_{i-1}[X]$, so α_i is algebraic over K_{i-1}. Hence by Theorem 3, $K_i = K_{i-1}(\alpha_i)$ is a finite extension of K_{i-1}. By induction, K_{i-1} is a number field, so Lemma 4 tells us that K_i is a number field. □

This gives us a way to construct lots of number fields, of which we have already seen several examples.

There is the following converse.

Lemma 6. If K is a number field, then K is isomorphic to $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for some algebraic numbers $\alpha_1, \ldots, \alpha_n$.

It is easy to show that $K = \mathbb{Q}(\beta_1, \ldots, \beta_n)$ for some $\beta_1, \ldots, \beta_n$ which are algebraic elements of the extension $K/\mathbb{Q}$. But the definition of algebraic numbers requires them to be in $\mathbb{C}$. So the hard part of the theorem is showing that every number field K can be embedded in $\mathbb{C}$, even if it was constructed by some abstract method which had nothing to do with $\mathbb{C}$.

4. Number fields and algebraic numbers

Lemma 6. If K is a number field, then K is isomorphic to $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for some algebraic numbers $\alpha_1, \ldots, \alpha_n$.

In particular, every number field is isomorphic to a subfield of $\mathbb{C}$.

Proof. Let $\beta_1, \ldots, \beta_n$ be a $\mathbb{Q}$-basis for K. Then $K = \mathbb{Q}(\beta_1, \ldots, \beta_n)$. By Lemma 2, $\beta_1, \ldots, \beta_n$ are algebraic elements of the extension $K/\mathbb{Q}$.

Let $K_i = \mathbb{Q}(\beta_1, \ldots, \beta_i)$. We shall prove by induction that K_i is isomorphic to a field of the form $L_i = \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ where $\alpha_1, \ldots, \alpha_n$ are algebraic numbers (in particular, $L_i \subseteq \mathbb{C}$).

Base case: $K_0 = \mathbb{Q}$. There is nothing to prove.

For $i \geq 1$: We have $K_i = K_{i-1}(\beta_i)$. Because β_i is algebraic over $\mathbb{Q}$, it is also algebraic over K_{i-1} ($\mu_{\mathbb{Q},\alpha_i} \in \mathbb{Q}[X] \subseteq K_{i-1}[X]$). Let μ_i be the minimal polynomial of α_i over K_{i-1}.

By induction, there is an isomorphism $\sigma_{i-1} \colon K_{i-1} \to L_{i-1} = \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}) \subseteq \mathbb{C}$. Let $\nu_i \in L_{i-1}[X]$ be the polynomial obtained by applying σ_{i-1} to the coefficients of μ_i. Then we can think of ν_i as a polynomial over $\mathbb{C}$, and it is non-constant. By the Fundamental Theorem of Algebra, ν_i has a root $\alpha_i \in \mathbb{C}$. Since $\nu_i(\alpha_i) = 0$ and ν_i is monic and irreducible over L_{i-1}, ν_i is the minimal polynomial of α_i over L_{i-1}.

By Theorem 3 (twice), we have isomorphisms

$$K_i = K_{i-1}(\beta_i) \cong K_{i-1}[X]/(\mu_i) \cong L_{i-1}[X]/(\nu_i) \cong L_{i-1}(\alpha_i) = L(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i).$$

□

The field of algebraic numbers.

Lemma 7. Let $\alpha, \beta \in \mathbb{C}$ be algebraic numbers. Then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and α/β (if $\beta \neq 0$) are also algebraic numbers.

Proof. $\mathbb{Q}(\alpha, \beta)$ is a number field by Lemma 5. Hence every element of $\mathbb{Q}(\alpha, \beta)$ is an algebraic number. But $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and α/β are all elements of $\mathbb{Q}(\alpha, \beta)$. □

This is quite incredible! In a simple example, we had to do some work before to show that $i + \sqrt{2}$ was algebraic (and more to find its minimal polynomial). For example, if α is a root of

$$X^{10000} + 5X^{73} + 2X^8 - 6X - 22$$

and β is a root of

$$X^{99999} + 777X^2 - 5$$

then there is a polynomial with rational coefficients which has $\alpha + \beta$ as a root. Finding this polynomial is a hard computation problem (can you guess what its degree might be?) but the theorem tells us that it exists.

Definition. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic number}\}$.

Corollary. $\overline{\mathbb{Q}}$ is a field.

Proof. Immediate corollary of Lemma 7. □

Question. Why is $\overline{\mathbb{Q}}$ not a number field?

Quadratic fields.

The simplest example of a number field is $\mathbb{Q}$. Indeed $\mathbb{Q}$ is the only number field of degree 1. (Why?)

The next simplest examples are quadratic fields. We will use these a lot in this course.

Definition. A **quadratic field** is a number field of degree 2.

We have already seen some examples: if $d \in \mathbb{Q}$ is not the square of a rational number, then $\mathbb{Q}(\sqrt{d})$ is a quadratic field. There is some redundancy here e.g.

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{18}) = \mathbb{Q}(\sqrt{1/2}) = \mathbb{Q}(\sqrt{9/8}) = \cdots$$

We can eliminate this by insisting that d is always a square-free integer.

Definition. $d \in \mathbb{Z}$ is **square-free** if it is not divisible by m^2 for any integer $m > 1$. (Note: 1 is square-free, 0 is not.)

In fact all quadratic fields have this form.

Proposition 8. Let K be a quadratic field. Then $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer $d \neq 1$.

Proof. Since $[K : \mathbb{Q}] = 2 > 1$, we can pick $\alpha \in K$ which is not in $\mathbb{Q}$. Then $\{1, \alpha, \alpha^2\}$ are linearly dependent over $\mathbb{Q}$ i.e. there exist $a, b, c \in \mathbb{Q}$ such that

$$a\alpha^2 + b\alpha + c = 0.$$

If $a = 0$ then $\alpha \in \mathbb{Q}$ giving a contradiction. Thus $a \neq 0$ and the quadratic formula gives

$$\alpha = \frac{-b \pm \sqrt{\Delta}}{2a}, \text{ where } \Delta = b^2 - 4ac \in \mathbb{Q}. \qquad (*)$$

Rearranging this, we see that $\sqrt{\Delta} = \pm(2a\alpha + b) \in K$.

Now write

$$\Delta = \frac{u}{v} = \frac{1}{v^2}uv$$

where $u, v \in \mathbb{Z}$. Then $uv \in \mathbb{Z}$ and $\sqrt{uv} = v\sqrt{\Delta} \in K$.

Finally we can write $uv = x^2y$ where x is an integer and u is a square-free integer (use the prime factorisation of uv). We get $\sqrt{y} = \frac{1}{x}\sqrt{uv} \in K$.

Note that $\sqrt{\Delta} \notin \mathbb{Q}$ (otherwise (*) would force $\alpha \in \mathbb{Q}$). Hence $\sqrt{y} \notin \mathbb{Q}$. So $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$.

By the Tower Law,

$$[K : \mathbb{Q}(\sqrt{y})] = [K : \mathbb{Q}]/[\mathbb{Q}(\sqrt{y}) : \mathbb{Q}] = 1$$

so $K = \mathbb{Q}(\sqrt{y})$. □

Furthermore, the square-free integer d such that $K = \mathbb{Q}(\sqrt{d})$ is unique – this is on example sheet 1.

Note that Proposition 8 does not generalise to higher-degree fields. For example a cubic field (i.e. a field of degree 3) does not have to have the form $\mathbb{Q}(\sqrt[3]{d})$. We will need some more theory before proving this.

5. Primitive element theorem, norm and trace

Cyclotomic fields.

Definition. Let n be a positive integer and let $\zeta_n = \exp(2\pi i/n)$. We call $\mathbb{Q}(\zeta_n)$ the **n-th cyclotomic field**.

Lemma 9. If $n = p$ is prime, then the minimal polynomial of ζ_p is $X^{p-1} + X^{p-2} + \cdots + X + 1$ and hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Proof. This is on the example sheet. You will need to use Eisenstein polynomials from Algebra 2.

(Note that there was a typo on the first version of the example sheet: it said $X^p + \cdots + 1$ where it should be $X^{p-1} + \cdots + 1$.) □

If n is not a prime, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ (the Euler φ-function). There is no general formula for the minimal polynomial of ζ_n when n is not prime, so this is harder to prove.

Primitive element theorem.

The primitive element theorem tells us that every extension of number fields is a simple extension. For example, we saw that $\mathbb{Q}(i, \sqrt{2})$ is a simple extension of $\mathbb{Q}$: it is equal to $\mathbb{Q}(i + \sqrt{2})$.

Lemma 10. Let K be a number field contained in $\mathbb{C}$. Let $f \in K[X]$ be an irreducible polynomial over K of degree d. Then f has d distinct roots in $\mathbb{C}$.

Proof. By the Fundamental Theorem of Algebra, we know that f has d roots in $\mathbb{C}$ counted with multiplicity. The problem is to show that f has no repeated roots.

Suppose for contradiction that $\alpha \in \mathbb{C}$ is a repeated root of f.

Let f' denote the derivative of f, and note that it also has coefficients in K. Since α is a repeated root of f, it is also a root of f'. Hence $X - \alpha$ is a common factor of f and f' in $\mathbb{C}[X]$. It follows that $\mathrm{HCF}(f, f')$ is a non-constant polynomial.

Now $\mathrm{HCF}(f, f')$ has coefficients in K (we can calculate it using Euclid's algorithm, and f, f' both have coefficients in K). But $\mathrm{HCF}(f, f')$ is a factor of f, it is non-constant, and

$$\deg(\mathrm{HCF}(f, f')) \leq \deg(f') = \deg(f) - 1.$$

This contradicts the hypothesis that f is irreducible over K. □

The name of the lemma is because it is related to the notion of "separable field extension" in Galois theory.

Note that Lemma 10 works only because number fields have characteristic zero – this is needed to ensure that $f' \neq 0$. (Over a field of characteristic p, the derivative of X^p is 0. Then the argument about the degree of the HCF would break down.) If you have done Galois theory, this is related to the idea of a separable extension (and the fact that every extension in characteristic zero is separable).

In order to prove the Primitive Element Theorem, we start with an extension generated by adjoining two elements. We can then build up other extensions by

induction on the number of elements we need to adjoin. The idea for $K(\alpha, \beta)$ is motivated by the example of $\mathbb{Q}(i + \sqrt{2})$: we try adjoining a linear combination of α and β. Just taking $\alpha + \beta$ does not always work so we have to be a little cleverer about which linear combination we choose.

Lemma. Let L/K be an extension of number fields such that $K = L(\alpha, \beta)$. Then there is some $\gamma \in L$ such that $L = K(\gamma)$.

Proof. Thanks to Lemma 6, we may assume that L (and hence also K) is a subfield of $\mathbb{C}$, allowing us to apply Lemma 10.

Let f, g be the minimal polynomials of α, β respectively over K. Let $\alpha_1, \ldots, \alpha_m$ be the roots of f and let $\beta_1, \ldots, \beta_n$ be the roots of g in $\mathbb{C}$. We may label the roots so that $\alpha_1 = \alpha$ and $\beta_1 = \beta$.

For any i and any $j \neq 1$, the equation

$$\alpha + c\beta = \alpha_i + c\beta_j$$

has a unique solution $c = c_{ij} \in \mathbb{C}$ (this is just solving a linear equation for c). Since K is infinite, we can choose $c \in K$ different from all the c_{ij} (there are only finitely many c_{ij} because $1 \leq i \leq m$, $2 \leq j \leq n$). Thus

$$\alpha + c\beta \neq \alpha_i + c\beta_j \tag{$\dagger$}$$

for all i and for all $j \neq 1$.

Let $\gamma = \alpha + c\beta$. We shall show that $L = K(\gamma)$. It is enough to show that $\beta \in K(\gamma)$ because then $\alpha = \gamma - c\beta \in K(\gamma)$ (because $c \in K$).

Consider the polynomial $h(X) = f(\gamma - cX) \in K(\gamma)[X]$. Observe that $h(\beta) = f(\alpha) = 0$.

If β' is any root of h other than β, we have $f(\gamma - c\beta') = 0$ and so $\gamma - c\beta' = \alpha_i$ for some i. The fact that c does not satisfy any of the equations ($\dagger$) implies that $\beta' \neq \beta_j$ for any $j = 2, \ldots, n$.

Thus the only common root of g and h is β. Looking at the factorisations of g and h in $\mathbb{C}[X]$, we conclude that $\mathrm{HCF}(g, h) = (X - \beta)^r$ for some r.

Because g is a minimal polynomial, it is irreducible over K. Therefore by Lemma 10, g has no repeated roots in $\mathbb{C}$, so in fact we must have $\mathrm{HCF}(g, h) = X - \beta$.

Since g and h both have coefficients in $K(\gamma)$, so does $\mathrm{HCF}(g, h)$. Thus $\beta \in K(\gamma)$. □

Theorem 11 (Primitive Element Theorem)**.** Let L/K be an extension of number fields. Then there is some $\gamma \in L$ such that $L = K(\gamma)$.

Proof. Write $L = K(S)$ for some finite set S (this is always possible: for example, let S be a K-basis of L). Induct on the size of S, applying the previous lemma to reduce the size by 1 repeatedly. □

Norm and trace.

Let K be a number field. We define two functions $K \to \mathbb{Q}$ which can be helpful in transforming questions about elements of K into questions about rational numbers.

Recall that K is $\mathbb{Q}$-vector space and for any α we can define a $\mathbb{Q}$-linear map $m_{K,\alpha}\colon K \to K$ by $m_{K,\alpha}(\beta) = \alpha\beta$.

Definition. The **trace** of α is $\mathrm{Tr}(m_{K,\alpha})$ – written $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.

The **norm** of α is $\det(m_{K,\alpha})$ – written $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$.

The notation (subscript $K/\mathbb{Q}$) reminds us that $\mathrm{Tr}_{K/\mathbb{Q}}$ and $\mathrm{Nm}_{K/\mathbb{Q}}$ are functions $K \to \mathbb{Q}$.

Note that you could generalise this: instead of always having $\mathbb{Q}$ as the base field, you could define $\mathrm{Tr}_{L/K}$ and $\mathrm{Nm}_{L/K}$ for any extension of number fields L/K. These would be functions $L \to K$. The definition is essentially the same but we won't need this generalisation in the course.

e.g. Let $K = \mathbb{Q}(\sqrt{d})$. We want to work out the norm and trace of $\alpha = a + b\sqrt{d}$. To do this, we will write $m_{K,\alpha}\colon K \to K$ as a matrix with respect to the basis $\{1, \sqrt{d}\}$. We get

$$m_{K,\alpha}(1) = a \cdot 1 + b \cdot \sqrt{d}, \quad m_{K,\alpha}(\sqrt{d}) = bd \cdot 1 + a \cdot \sqrt{d}$$

so the matrix of $m_{K,\alpha}$ (with respect to this basis) is

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}.$$

Thus

$$\mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a.$$
$$\mathrm{Nm}_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - b^2 d,$$

6. Characteristic polynomial, embeddings

Lemma 12. The trace is additive and the norm is multiplicative. In other words, for all α, β in K, we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha+\beta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta),$$
$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha\beta) = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\,\mathrm{Nm}_{K/\mathbb{Q}}(\beta).$$

Proof. Observe that $m_{K,\alpha+\beta} = m_{K,\alpha} + m_{K,\beta}$ and $m_{K,\alpha\beta} = m_{K,\alpha}m_{K,\beta}$. Thus the lemma follows from the properties of trace and determinant of linear maps. □

Characteristic polynomials.

Let V be a $\mathbb{Q}$-vector space and let $f\colon V \to V$ be a $\mathbb{Q}$-linear map. Recall that the **characteristic polynomial** of f is the polynomial

$$\chi_f(X) = \det(XI - f) \in \mathbb{Q}[X].$$

This polynomial is monic of degree $n = \dim(V)$. We can read off the determinant and trace of f from the coefficients of the characteristic polynomial: if $\chi_f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, then

$$\mathrm{Tr}(f) = -a_{n-1}, \quad \det(f) = (-1)^n a_0. \tag{*}$$

According to the Cayley–Hamilton theorem, $\chi_f(f) = 0$.

Consequently we can read off the norm and trace of $\alpha \in K$ from the characteristic polynomial of $m_{K,\alpha}$, which we denote $\chi_{K,\alpha}$.

Lemma 13. Let $K = \mathbb{Q}(\alpha)$. Then the characteristic polynomial of $m_{K,\alpha}\colon K \to K$ is equal to the minimal polynomial of α over $\mathbb{Q}$.

Proof. Let $\chi_{K,\alpha}(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ denote the characteristic polynomial of $m_{K,\alpha}$. By the Cayley–Hamilton theorem, $\chi_{K,\alpha}(m_{K,\alpha}) = 0$. In other words,

$$m_{K,\alpha}^n + a_{n-1}m_{K,\alpha}^{n-1} + \cdots + a_1 m_{K,\alpha} + a_0 = 0$$

(in the ring of $\mathbb{Q}$-linear maps $K \to K$). Applying both sides to $1 \in K$, and noting that $m_{K,\alpha}^i(1) = \alpha^i$, we get

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

or in other words $\chi_{K,\alpha}(\alpha) = 0$.

Furthermore $\chi_{K,\alpha} \in \mathbb{Q}[X]$, $\chi_{K,\alpha}$ is monic and $\deg(\chi_{K,\alpha}) = [K:\mathbb{Q}] = \deg(\mu_{\mathbb{Q},\alpha})$ (the latter holds because $K = \mathbb{Q}(\alpha)$). Hence by Lemma 1, $\chi_{K,\alpha} = \mu_{\mathbb{Q},\alpha}$. □

Note that the characteristic polynomial $\chi_{K,\alpha}$ depends on K as well as α. The following lemma tells us how.

Lemma 14. Let L/K be an extension of number fields and let $\alpha \in K$. Let $\chi_{K,\alpha}$ and $\chi_{L,\alpha}$ be the characteristic polynomials of $m_{K,\alpha}\colon K \to K$ and $m_{L,\alpha}\colon L \to L$ respectively. Then

$$\chi_{L,\alpha} = \chi_{K,\alpha}^{[L:K]}.$$

Proof. Let $\theta_1, \ldots, \theta_r$ be a $\mathbb{Q}$-basis for K and let $M_{K,\alpha}$ be the matrix of $m_{K,\alpha}$ with respect to this basis. Let $\phi_1, \ldots, \phi_s$ be a K-basis for L. By the Tower Law, a $\mathbb{Q}$-basis for L is given by

$$\theta_1\phi_1, \theta_2\phi_1, \ldots, \theta_r\phi_1,\ \theta_1\phi_2, \ldots, \theta_2\phi_r,\ \ldots,\ \theta_1\phi_s, \ldots, \theta_r\phi_s.$$

We can calculate that

$$m_{L,\alpha}(\theta_i\phi_j) = \alpha\theta_i\phi_j = m_{K,\alpha}(\theta_i) \cdot \phi_j.$$

Thus $m_{L,\alpha}(\theta_i\phi_j)$ lies in the $\mathbb{Q}$-space spanned by $\theta_1\phi_j, \ldots, \theta_r\phi_j$ (for fixed j), and the coefficients needed to express $m_{L,\alpha}(\theta_i\phi_j)$ as a combination of these basis vectors are the same as the coefficients needed to express $m_{K,\alpha}(\theta_i)$ as a combination of $\theta_1, \ldots, \theta_r$; in other words, they are entries of $M_{K,\alpha}$.

Consequently the matrix for $m_{L,\alpha}$ with respect to the basis $\{\theta_i\phi_j\}$ is block diagonal with blocks that are copies of $M_{K,\alpha}$:

$$M_{L,\alpha} = \begin{pmatrix} M_{K,\alpha} & 0 & \cdots & 0 \\ 0 & M_{K,\alpha} & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & M_{K,\alpha} \end{pmatrix}$$

There is one block for each ϕ_j i.e. s blocks. This is consistent with the fact that $M_{K,\alpha}$ is an $s \times s$ matrix and $M_{L,\alpha}$ is an $rs \times rs$ matrix.

The characterstic polynomial of a block diagonal matrix is the product of the characteristic polynomials of the blocks (because the same thing holds for determinants). Thus

$$\chi_{L,\alpha}(X) = \chi_{K,\alpha}(X)^s. \qquad \square$$

Corollary 15. Let L/K be an extension of number fields. If $\alpha \in K$, then

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = [L : K]\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha),$$
$$\mathrm{Nm}_{L/\mathbb{Q}}(\alpha) = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)^{[L:K]}.$$

Proof. Let $r = [K : \mathbb{Q}]$ and $s = [L : K]$. Write

$$\chi_{K,\alpha}(x) = X^r + a_{r-1}X^{r-1} + \cdots + a_1X + a_0,$$
$$\chi_{L,\alpha}(x) = X^{rs} + b_{rs-1}X^{rs-1} + \cdots + b_1X + b_0.$$

By Lemma 14, we have $\chi_{L,\alpha} = \chi_{K,\alpha}^s$. Expanding this out and comparing coefficients, we see that

$$b_{rs-1} = sa_{r-1}, \quad b_0 = a_0^s.$$

The corollary now follows from (*). $\square$

By combining Lemmas 13 and 14, we can work out the characteristic polynomial of an arbitrary $\alpha \in K$ in terms of the minimal polynomial:

$$\chi_{K,\alpha} = \mu_{\mathbb{Q},\alpha}^{[K:\mathbb{Q}(\alpha)]}$$

It can be useful to apply this in reverse: by choosing a basis for K, we can work out the characteristic polynomial $\chi_{K,\alpha}$. This must be a power of an irreducible polynomial, which will be the minimal polynomial of α.

Embeddings of number fields.

Definition. Let K be a number field. An **embedding** of K is a field homomorphism $\sigma\colon K \to \mathbb{C}$.

Lemma 16. Any homomorphism of fields $\sigma\colon K \to L$ is injective.

Proof. The kernel of σ is an ideal in K. Since K is a field, its only ideals are 0 and K. But $\ker(\sigma) \neq K$ because $\sigma(1) = 1 \neq 0$. □

Lemma 17. Let K be a number field and let $\sigma\colon K \to \mathbb{C}$ be an embedding. Then $\sigma(a) = a$ for all $a \in \mathbb{Q}$.

Proof. By the definition of a ring homomorphism, $\sigma(1) = 1$ and $\sigma(0) = 0$. For any positive integer n, we have

$$\sigma(n) = \sigma(1 + \cdots + 1) = \sigma(1) + \cdots + \sigma(1) = 1 + \cdots + 1 = n.$$

Furthermore $\sigma(-n) = -\sigma(n) = n$.

Finally, any rational number can be written as m/n where $m, n \in \mathbb{Z}$, and $\sigma(m/n) = \sigma(m)/\sigma(n) = m/n$. □