

Algebraic Number Theory

Vinesh Ramgi

June 28, 2019

Abstract

What did the number theorist say as he drowned?

Log, log, log, log....

For an up to date version of this pdf, check my GitHub :)

<https://github.com/vrvinny/algebraic.nt>

Contents

1	Introduction/Review	4
1.1	Introduction	4
1.2	Definitions and proofs	5
2	Materials from other courses on rings, ideals and fields	7
2.1	Quotient Rings	8
2.2	1st Isomorphism Theorem for Rings	9
2.3	Maximal Ideals	9
2.4	Field extensions	10
2.5	Finding Minimal Polynomials	11
2.6	Eisenstein's Criterion	11
2.7	Roots of Unity	12
2.8	Tower Law	13
2.9	Primitive Element Theorem	14
2.10	Conjugates and Complex Field Embeddings	14
2.11	Galois Separability Lemma	14

1 Introduction/Review

1.1 Introduction

This is the study of certain rings, numbers called algebraic integers, e.g.

- Quadratic rings $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$
- Cyclotomic rings $\mathbb{Z}[\zeta_n] \implies y = e^{2\pi i/n}$
- $\mathbb{Z}[z\sqrt{2}] = \{x + y^3\sqrt{2} + z^3\sqrt{z^2}\} \ x, y, z \in \mathbb{Z}$

Definition 1.1. A Diophantine equation is an equation of the form $f(x_1, \dots, x_n) = 0$ where f is a polynomial with coefficients in \mathbb{Z}

We'll usually be interested in solution in integers (or maybe rational numbers), for example, Pell's equation- $x^2 - dy^2 = 1$, or $N(A) = n$ where $A = x + y\alpha$, $\alpha = \{\sqrt{d}, \frac{1+\sqrt{d}}{2}\}$.

In general Diophantine equations are hard, Matiyasevich's theorem shows Diophantine equations are as hard as any mathematical question. In spite of this, there are some Diophantine equations for which we have methods for solving, e.g. *What are the integer solutions of $x^3 = y^2 + y = y(y+1)$?*

Since $y, y+1$ are both coprime and their product is a cube, both y and $y+1$ are a cube which implies $y = 0, -1$. So we have two solutions, $(0, 0), (0, -1)$. To do this we used this lemma:

Lemma 1.2. *Descent Lemma*

Let R be a ring be a unique factorisation domain. Suppose $a, b, c \in R$ and $a^n = bc$. If b, c are coprime in R then $b = u^{r^n}$, $c = vs^n$ where u, v are units in R .

Another example, $x^3 = y^2 + 1$:

Problem, $y^2 + 1$ doesn't factorise in \mathbb{Z} but it does factorise in $\mathbb{Z}[i] \implies x^3 = (y+i)(y-i)$. We want to use the Descent lemma to solve the equation.

- $\mathbb{Z}[i]$ is a unique factorisation domain
- Are $y+i$ and $y-i$ coprime in $\mathbb{Z}[i]$?

Suppose $p \in \mathbb{Z}[i]$ is an irreducible common factor of $y+i, y-i$. If $p|y+i$ and $p|y-i \implies p|(y+i) - (y-i) \implies p|2i$. This means the norms also divide each other, $N(p)|N(2i) \implies N(p)|4$.

$N(p) \neq \pm 1$ because p isn't a unit, therefore, $2|N(p)|N(y+i) \implies N(y+i) = y^2 + 1 = x^3$, so $2|x^3$.

Since 2 is a prime, $2|x \implies x^3 \equiv 0 \pmod{8}$. This implies $y^2 + 1 \equiv 0 \pmod{8}$

y	$y^2 \pmod{8}$
0	0
± 1	1
± 2	4
± 3	1
4	0

Since the equation has no solutions, $y^2 + 1 \equiv 0 \pmod{8}$ has no solutions.

So $y + i, y - i$ are coprime in $\mathbb{Z}[i]$.

$\therefore y + 1 = uA^3$ with $u \in \mathbb{Z}[i]^\times$, $A \in \mathbb{Z}[i]$ with $u = \pm 1$ or $\pm i$

So in fact

$$\begin{aligned} y + i &= (r + si)^3 \quad r, s \in \mathbb{Z} \\ &= r^3 + 3ir^2s - 3rs^2 - is^3 \\ &= r^3 - 3rs^2 + i(3r^2s - s^3) \end{aligned}$$

Organising the terms gives a new Diophantine equation:

$$1 = 3r^2s - s^3 \qquad y = r^3 - 3rs^2$$

We can solve the new equation:

$$1 = (3r^2 - s^2)s \implies s = \pm 1$$

$$\text{If } s = 1 \implies 3r^2 - 1 = 1 \nmid$$

$$\text{If } s = -1 \implies 3r^2 - 1 = -1 \implies r = 0 \quad \text{so } (r, s) = (0, -1)$$

This implies $x = 1, y = 0$ so $(1, 0)$ is the only solution in integers.

This motivates the question: which rings are unique factorisation domains? More specifically which rings of algebraic integers are unique factorisation domains?

1.2 Definitions and proofs

A ring is a set R with two operations $+$ & \times . $(R, +)$ is an abelian group with identity element 0. \times is commutative, associative and has identity 1. $x(y + z) = xy + xz \quad \forall x, y, z \in R$

An element $x \in R$ is:

- a unit if $\exists x^{-1} \in R$ such that $xx^{-1} = 1$
- reducible if $x = yz$ where y, z not units
- irreducible otherwise

For examples, in \mathbb{Z} , units are ± 1 , irreducible elements are $\pm p$ for prime numbers p .

Definition 1.3. A ring R is an integral domain if $xy = 0 \implies x = 0$ or $y = 0$

Lemma 1.4. Cancellation property: If R is an integral domain, if $x \neq 0$ then $xy = xz \implies y = z$

Proof.

$$\begin{aligned} xy = xz &\implies x(y - z) = 0 \text{ and since } x \neq 0 \\ &\implies y - z = 0 \\ &\implies y = z \end{aligned}$$

□

A ring R is a unique factorisation domain if:

- R is an integral domain
- If $x \in R$ and $x \neq 0$ then $x = Up_1 \dots p_r$ with $U \in R^\times$ and P_i irreducible

Suppose $p_1 \dots p_r = q_1 \dots q_s$ with p_i, q_i irreducible then $r = s$ and we can renumber so that $q_i = Up_i$ with $U \in R^\times$.

The 3^{rd} condition is equivalent to if $p \in R$ is irreducible and $p|ab$ then $p|a$ or $p|b$.

Lemma 1.5. *Descent Lemma: Let R be a UFD (Unique Factorisation Domain) and let $a, b, c \in R$ with $a^n = bc$ and b, c coprime. Then $b = ur^n$ and $c = vs^n$ with $u, v \in R^\times$*

Proof. If a is a unit then b and c are units, so the result is true.

If $a = 0$ then $b = 0$ or $c = 0$.

WLOG assume $b = 0 = 1 * 0^n$. But b and c are coprime $\implies c$ must be a unit (since it is a common factor of b and c).

In other cases $a = p_1 \dots p_r$ with p_i irreducible. So

$$\begin{aligned} b &= (\text{a unit}) * p_1^{s_1} \dots p_r^{s_r} & s_i + t_i &= n \forall i \\ c &= (\text{a unit}) * p_1^{t_1} \dots p_r^{t_r} \end{aligned}$$

But we're assuming b, c are coprime so:

\implies each s_i is either 0 or n

$\implies b = (\text{a unit}) * (\text{some } n^{th} \text{ power}) \implies c = (\text{a unit}) * (\text{some } n^{th} \text{ power})$ □

Reminder about quadratic rings

Let $d \neq 1$ be a square free integer and $\mathbb{Z}[\alpha] = \{x + y\alpha : x, y \in \mathbb{Z}\}$

$$\alpha = \alpha_d = \begin{cases} \sqrt{d} & d \not\equiv 1 \pmod{4} \\ \frac{1 + \sqrt{d}}{2} & d \equiv 1 \pmod{4} \end{cases}$$

If $A = x + y\sqrt{d}$ then $\bar{A} = x - y\sqrt{d}$ and $N(A) = A\bar{A} = x^2 - dy^2$.

Similarly $N(x + y\frac{1+\sqrt{d}}{2}) = x^2 + xy + \frac{1-d}{4}y^2$.

The ring $\mathbb{Z}[\alpha]$ is norm-Euclidean if for all $A, B \in \mathbb{Z}[\alpha]$ with $B \neq 0$, $\exists Q, R \in \mathbb{Z}[\alpha]$ such that $A = QB + R$ and $|N(R)| < |N(B)|$.

Proposition 1.6. *If $\mathbb{Z}[\alpha]$ is norm-Euclidean then $\mathbb{Z}[\alpha]$ is a UFD.*

Proof. (Sketch)

We'll show that if $p \in \mathbb{Z}[\alpha]$ is irreducible and $p|AB$ then $p|A$ or $p|B$.

If $p \nmid A$ then $\text{hcf}(A, p) = 1 \implies 1 = HA + KP$ by the Euclidean algorithm.

$$B = \underbrace{HAB}_{\text{multiple of } p} + \underbrace{KPB}_{\text{multiple of } p} \implies p|B$$

□

Theorem 1.7. *Disappointing Theorem: $\mathbb{Z}[\alpha_d]$ is norm-Euclidean in the following cases $d = 2, 3, 5, 13, -1, -2, -3, -7, -11$. Conjecturally there are infinitely many real quadratic rings which are UFD.*

2 Materials from other courses on rings, ideals and fields

Mainly from Galois Theory, Commutative Algebra and Groups and Rings. In this course,

- All rings are commutative with 1
- A field is a ring with $1 \neq 0$
- If $x \neq 0$, x is a unit

Definition 2.1. An ideal I in a ring R is a subset of R such that:

- $(I, +)$ is a subgroup of R
- $\forall x \in R, y \in I \implies xy \in I$

Examples: If $x \in R$ then we define $(x) = \{xy : y \in R\}$. This set (x) is an ideal in R .

Definition 2.2. Ideals of the form (x) are called principal ideals. (x) is the principle ideal generated by x .

$(x_1, \dots, x_n) = \{x_1y_1 + \dots + x_ny_n : y_i \in R\}$ this is also an ideal.

E.g. in \mathbb{Z} $(4, 6) = (2)$ and in general $(n, m) = (\text{hcf}(n, m))$

Definition 2.3. A principal ideal domain is an integral domain such that all ideals are principal. A Noetherian ring is a ring in which ideals are finitely generated.

To show that $(x_1, \dots, x_n) \subseteq I$, it is equivalent to showing $x_1, \dots, x_n \in I$

E.g. in \mathbb{Z} $(4, 6) = (2)$

Proof.

$$\begin{array}{ll} (4, 6) \subseteq (2) & (2) \subseteq (4, 6) \\ 4 = 2 * 2 \in (2) & 2 = 2 * 4 + (-1) * 6 \in (4, 6) \\ 6 = 2 * 3 \in (2) & \end{array}$$

□

Definition 2.4. A principal ideal domain is an integral domain in which every ideal is principal

E.g. \mathbb{Z} is a PID

Proof. Suppose $I \subseteq \mathbb{Z}$ is an ideal.

If $I = \{0\}$ then $I = (0)$.

If $I \neq \{0\}$ choose $x \in I$ with $|x|$ as small as possible with $x \neq 0$.

Claim $I = (x)$, $x \in I \implies x \subseteq I$.

Conversely, suppose $y \in I$ with $y = qx + r$ such that $|r| < |x|$. This means that $r = y - qx \in I \implies r = 0 \implies y = qx \in (x)$ which means $I \subseteq (x)$. \square

E.g. If $\mathbb{Z}[\alpha]$ is a norm-Euclidean quadratic ring then $\mathbb{Z}[\alpha]$ is a PID.

Proof. Replace $|x|$ by $|N(A)|$ for $A \in \mathbb{Z}[\alpha]$. \square

E.g. If k is a field then $k[x]$ is a PID.

Proof. Replace $|x|$ by $\deg(f)$ for $f \in k[x]$. \square

2.1 Quotient Rings

Let I be an ideal in R , we'll say $x = y \in (I)$ if $x - y \in I$.

$R/I = \{\text{Congruency classes of elements of } R\}$

Lemma 2.5. If $x \equiv x' \pmod{I}$ and $y \equiv y' \pmod{I}$ then $x + y \equiv x' + y' \pmod{I}$ and $xy \equiv x'y' \pmod{I}$

This means we can make R/I into a ring.

Proof. If $x - x' \in I$ and $y - y' \in I$ then:

$$(x + y) - (x' + y') = (x - x') + (y - y') \in I$$

$$\begin{aligned} xy - x'y' &= xy - xy' + xy' - x'y' \\ &= x(y - y') + (x - x')y \in I \end{aligned}$$

\square

E.g. If $R = \mathbb{Z}$, $I = (n)$ and $x \equiv x' \pmod{I} \Leftrightarrow x \equiv x' \pmod{n} \implies R/I = \mathbb{Z}/n$

E.g. If k is a field and $f \in k[x]$ with degree d and $I = (f)$, every element of $k[x]$ is congruent to a unique polynomial of degree $< d$. (The remainder after dividing by f).

$\therefore R/I = \{a_0 + a_1x + \cdots + a_{d-1}x^{d-1} : a_i \in k\}$

Definition 2.6. Let R and S be rings. A ring homomorphism is a function $\phi : R \rightarrow S$ such that:

- $\phi(x + y) = \phi(x) + \phi(y)$
- $\phi(xy) = \phi(x)\phi(y)$

- $\phi(1_R) = 1_S$

$\ker(\phi) = \{x \in R : \phi(x) = 0\}$ and $\ker(\phi)$ is an ideal of R (trivial to prove)
 $\text{im}(\phi) = \{\phi(x) : x \in R\}$ and $\text{im}(\phi)$ is a subring of S

2.2 1st Isomorphism Theorem for Rings

Let $\phi : R \rightarrow S$ be a ring homomorphism. Then there is an isomorphism:

$$R/\ker(\phi) \cong \text{im}(\phi) \text{ by the mapping } (x \text{ mod } \ker(\phi)) \rightarrow \phi(x)$$

2.3 Maximal Ideals

Definition 2.7. Let R be a ring. An ideal $M \subseteq R$ is maximal if:

- $M \neq R$
- If $M \subseteq I \subseteq R$ with I an ideal then $I = M$ or $I = R$

Proposition 2.8. Suppose R is a PID, an ideal (x) is maximal if and only if x is irreducible.

Proof. Algebra 4 □

Note that the difference between a field and a ring is that if $x \neq 0$ then $xx^{-1} = 1$ and $1 \neq 0$.

Proposition 2.9. In any ring R , M is maximal if and only if R/M is a field

Proof. (\implies) Assume M is maximal therefore $M \neq R$ and $1 \notin M$ and $1 \not\equiv 0 \pmod{M}$.

Assume $x \not\equiv 0 \pmod{M}$, let I be the ideal generated by M and x , then $I \supsetneq M$ which means $I = R$.

$$I = \{m + xy : m \in M, y \in R\} \implies 1 = m + xy \text{ and } 1 \equiv xy \pmod{M}$$

(\impliedby) Assume R/M is a field so $1 \not\equiv 0 \pmod{M}$.

$\therefore 1 \notin M$ so $M \neq R$.

Suppose $M \subsetneq I$, want to show $I = R$. Choose $x \in I, x \notin M$ so $x \not\equiv 0 \pmod{M}$

So $\exists y$ such that $xy \equiv 1 \pmod{M}$ and by the definition of existence of x^{-1} , $1 \in I \implies I = R$ □

Corollary 2.10. Let k be a field and $f \in k[x]$, then $k[x]/(f)$ is a field if f is irreducible over k

Proof. f irreducible $\iff (f)$ is maximal $\iff k[x]/(f)$ is a field.

(Polynomial ring is ideal) □

2.4 Field extensions

Definition 2.11. If k and l are fields with $k \subseteq l$ then k is a subfield of l .
 l is called a field extension of k , e.g. $\mathbb{R} \subseteq \mathbb{C}$

When l is an extension of k , we can think of l as a vector space over k .

E.g. \mathbb{C} has basis $\{1, i\}$ as a vector space over \mathbb{R}

The degree of the extension $[l : k]$ is the dimension of l as a vector space over k

E.g. $[\mathbb{C} : \mathbb{R}] = 2$

E.g. $\mathbb{Q}(i) = \{x + iy : x, y \in \mathbb{Q}\}$

This is an extension of \mathbb{Q} with basis $\{1, i\} \implies [\mathbb{Q}(i) : \mathbb{Q}] = 2$

E.g. Let $f \in \mathbb{Q}[x]$ be irreducible $\implies \mathbb{Q}[x]/(f) = \{a_0 + a_1x + \dots + a_{d-1}x^{d-1}\}$ is a field.

This is an extension of \mathbb{Q} and has degree $d = \deg(f)$.

$\{1, x, \dots, x^{d-1}\}$ is a basis, so $[\mathbb{Q}[x]/(f) : \mathbb{Q}] = d = \deg(f)$.

Notation: Let l be an extension of k and let $\alpha \in l$, then:

Definition 2.12. α is called "algebraic over k " if there exists a non-zero $f \in k[x]$ such that $f(\alpha) = 0$. Otherwise α is transcendental.

E.g. $\sqrt{2}$ is algebraic over \mathbb{Q} since it is a root of $x^2 - 2$

For any $\alpha \in l$ $k[\alpha] = \{g(\alpha) : g \in k[x]\}$, the ring generated by k and α .

$k(\alpha) = \{\frac{g(\alpha)}{h(\alpha)} : g, h \in k[x], h(\alpha) \neq 0\}$, the field generated by k and α .

Proposition 2.13. Let α be algebraic over k . Then there is a unique monic polynomial $m(x) \in k[x]$ such that:

- $m(\alpha) = 0$
- $f(\alpha) = 0 \iff m|f$

m is the only monic irreducible polynomial over k such that $m(\alpha) = 0$.

Definition 2.14. This polynomial is called the minimal polynomial of α over k

E.g. i is algebraic over \mathbb{R} with minimal polynomial $x^2 + 1$

i is algebraic over \mathbb{Q} with minimal polynomial $x^2 + 1$

i is algebraic over \mathbb{C} with minimal polynomial $x - i$

Corollary 2.15. Let α be algebraic over k , then $k[\alpha] = k(\alpha)$, i.e. $k[\alpha]$ is a field and there is an isomorphism

$$\begin{aligned} k[x]/(m) &\cong k(\alpha) \\ (g(x) \bmod m) &\mapsto g(\alpha) \\ a_0 + a_1x + \dots + a_{d-1}x^{d-1} &\mapsto a_0 + a_1\alpha + \dots + a_{d-1}\alpha^{d-1} \end{aligned}$$

where m is the minimal polynomial and has degree d .

$\{1, \alpha, \dots, \alpha^{d-1}\}$ forms a basis for $k(\alpha)$ and $[k(\alpha) : k] = d = \deg(m)$

Proof. We have a homomorphism (surjective) $k[x] \rightarrow k[\alpha] \implies k[x]/(m) \cong k[\alpha]$ and $g \mapsto g(\alpha)$. (Field because m is irreducible)

Kernel = $\{g : g(\alpha) = 0\} = (m)$, therefore $k[\alpha] = k(\alpha)$ the isomorphism takes $(g(x) \bmod m)$ to $g(\alpha)$.

$\{1, x, \dots, x^{d-1}\}$ is a basis for $k[x]/(m)$

So $\{1, \alpha, \dots, \alpha^{d-1}\}$ is a basis for $k(\alpha)$ □

E.g. i is algebraic over \mathbb{R} with minimal polynomial $x^2 + 1$

$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{R}(i) = \mathbb{C}$ with the map $a + bx \mapsto a + bi$ $a, b \in \mathbb{R}$

Similarly $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i)$ with $a, b \in \mathbb{Q}$ with the map $a + bx \mapsto a + bi$

E.g. $\alpha = \sqrt[3]{2}$ This is a root of $x^3 - 2$ and so α is algebraic (over \mathbb{Q}).

$\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\alpha)$ with the mapping $a + bx + cx^2 \mapsto a + b\alpha + c\alpha^2$.

The degree of the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ with $\{1, \alpha, \alpha^2\}$ a basis for $\mathbb{Q}(\alpha)$ over \mathbb{Q} .

2.5 Finding Minimal Polynomials

We need methods to check that a polynomial is irreducible over \mathbb{Q} .

Lemma 2.16. *Gauss Lemma: Suppose $f \in \mathbb{Z}[x]$ and $f = gh$ $g, h \in \mathbb{Q}[x]$, then there exists $c \in \mathbb{Q}^\times$ such that cg and $c^{-1}h$ are in $\mathbb{Z}[x]$.*

Lemma 2.17. *Monic Gauss Lemma: Let $f \in \mathbb{Z}[x]$ be monic, if $f = gh \in \mathbb{Q}[x]$ both monic then $g, h \in \mathbb{Z}[x]$.*

Corollary 2.18. *If $f \in \mathbb{Z}[x]$ is monic the f is irreducible over $\mathbb{Q} \iff$ irreducible over \mathbb{Z}*

Corollary 2.19. *Let $f \in \mathbb{Z}[x]$ be monic. Let \bar{f} be the reduction of $f \bmod n$, i.e. $\bar{f} \in (\mathbb{Z}/n)[x]$. If \bar{f} is irreducible then f is irreducible over \mathbb{Z} and over \mathbb{Q} . Note that n doesn't need to be prime*

2.6 Eisenstein's Criterion

Let $f \in \mathbb{Z}[x]$ and let p be prime. Let $f(x) = a_d x^d + \dots + a_0$, if $p \nmid a_d$ and $f(x) \equiv a_d x^d \pmod{p}$ and let $f(0) \not\equiv 0 \pmod{p^2}$ then f is irreducible over \mathbb{Z}/p^2 and over \mathbb{Q} .

E.g. $\alpha = 10^{\frac{1}{11}} \implies \alpha^{11} = 10$.

α is a root of $x^{11} - 10$

$x^{11} - 10$ is irreducible by Eisenstein's Criterion (either with $p = 2$ or $p = 5$)

So $m_\alpha(x) = x^{11} - 10$

E.g. $\alpha = 2^{\frac{2}{3}}$

$\alpha^3 = 4$

α is a root of $m(x) = x^3 - 4$

To show that m is the minimal polynomial, we must show that m is irreducible.

$$m(x+1) = x^3 + 3x^2 + 3x - 3$$

$m(x+1)$ is irreducible by Eisenstein's criterion with $p = 3 \implies m(x)$ is irreducible.

E.g. $\alpha = 3^{\frac{2}{3}}$

$$\alpha^3 - 9 = 0$$

α is a root of $m(x) = x^3 - 9$. Note that $\deg(m) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. To show that m is the minimal polynomial it's sufficient to show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 3$

$$\alpha = 3\beta \text{ where } \beta = 3^{\frac{1}{3}} = \frac{1}{3}\alpha^2 \text{ so } \beta \in \mathbb{Q}(\alpha) \implies \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$$

β has minimal polynomial $x^3 - 3$ (by Eisenstein's criterion)

$$\therefore [\mathbb{Q}(\beta) : \mathbb{Q}] = 3$$

$$\therefore m(\alpha) \text{ has degree } \geq 3$$

$$\therefore m_\alpha = x^3 - 9$$

Alternatively suppose $x^3 - 9$ factorises over \mathbb{Q} . By the Monic Gauss lemma, $x^3 - 9 = (x - a)(x^2 + bx + c)$. By comparing coefficients, $ac = 9$, which means $a = \pm 1$ or ± 3 or ± 9 and $a^3 = 9$ because a is a root. \nexists

E.g. $\alpha = \sqrt{2} + \sqrt{3}$

$$\begin{aligned} \alpha^2 &= 2 + 2\sqrt{6} + 3 & (\alpha^2 - 5) - 24 &= 0 \\ &= 5 + 2\sqrt{6} \end{aligned}$$

So α is a root of $m(x) = x^4 - 10x^2 + 1$

Suppose $m(x) = (x - a)(x^3 + bx^2 + cx + d)$ with $a, b, c, d \in \mathbb{Z}$

a is a root of m and a is a factor of $m(0) = 1$ so $a = \pm 1$ which is a contradiction since $m(\pm 1) = -8 \neq 0$.

The other possible factorisation is $m(x) = (x^2 + ax + b)(x^2 + cx + d)$. Comparing coefficients:

$$\begin{aligned} 0 &= a + c \\ -10 &= b + d + ac & c &= -a & a^2 &= 10 \pm 2 = 8 \text{ or } 12 \nexists \\ 0 &= ad + bc \\ 1 &= bd & b &= d = \pm 1 \end{aligned}$$

2.7 Roots of Unity

Let n be a positive integer. An n^{th} root of unity is a complex number ζ such that $\zeta^n = 1$. A primitive n^{th} root of unity is an n^{th} root of unity which is not a d^{th} root of unity for any $d < n$.

n^{th} root of unity: $e^{2\pi i \frac{a}{n}}$ for $a = 0, 1, \dots, n-1$

Primitive n^{th} root of unity $e^{2\pi i \frac{a}{n}}$ for $a \in (\mathbb{Z}/n)^\times$.

There are $\phi(n)$ primitive n^{th} roots of unity.

The n^{th} cyclotomic polynomial is $\Phi_n(x) = \prod_{\substack{\text{Primitive } n^{\text{th}} \\ \text{roots of unity}}} (x - \zeta)$

$$\deg(\Phi_n(x)) = \phi(n)$$

Lemma 2.20. For any n : $\prod_{d|n} \Phi_d(x) = x^n - 1$. We can use this to calculate Φ_n .

E.g. If p prime then $\Phi_1(x)\Phi_p(x) = x^p - 1$.

$$\text{So } \Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + \dots + x^{p-1}$$

Corollary 2.21. $\Phi_n(x)$ has coefficient in \mathbb{Z} .

Remark: If ζ is a primitive n^{th} root of unity then ζ is a root of Φ_n

Theorem 2.22. Each Φ_n is irreducible over \mathbb{Q} . So Φ_n is the minimal polynomial of a primitive n^{th} root of unity.

2.8 Tower Law

Theorem 2.23. Suppose $k \subseteq l \subseteq m$ be fields. Then $[m : k] = [m : l] * [l : k]$

Proof. Sketch: Let $\{b_1, \dots, b_n\}$ be a basis for l as a vector space over k .

Let $\{c_1, \dots, c_m\}$ be a basis for m over k .

Then $\{b_i, c_j\}$ is a basis for m over k . □

E.g. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $x^2 - 2$ is the minimal polynomial.

The minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is a factor of $x^2 - 3$ so degree is 1 or 2.

From the Tower theorem, we know $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2$ or 4.

$$\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\alpha}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

deg 4 since
 α has
minimal
polynomial
 $x^4 - 10x^2 + 1$

By the Tower law $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ is a multiple of 4.

$$\therefore [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

$$\therefore [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$$

$x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$

Also $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\alpha)] = 1$ i.e. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\alpha)$

This is an example of:

2.9 Primitive Element Theorem

Theorem 2.24. Suppose k is an extension of \mathbb{Q} of finite degree then there exists $\alpha \in k$ such that $k = \mathbb{Q}(\alpha)$

Proof. Sketch: k has only finitely many subfields. Choose an $\alpha \in k$ which is not in any of the proper subfields.

$\mathbb{Q}(\alpha)$ is not contained in a proper subfield of k but $\mathbb{Q}(\alpha)$ is a subfield of k , therefore $\mathbb{Q}(\alpha) = k$. \square

2.10 Conjugates and Complex Field Embeddings

Let α, β be algebraic numbers. Then α and β are conjugates if $m_\alpha = m_\beta$. They have the same minimal polynomial over \mathbb{Q} .

E.g. $\alpha = i, \beta = -i$ both have minimal polynomial $x^2 + 1$.

E.g. $\zeta = e^{2\pi i \frac{1}{100}}$ This is a conjugate of ζ^3 , both have minimal polynomial Φ_{100} .

E.g. $\sqrt{2} + \sqrt{3}$ has conjugates $\pm\sqrt{2} \pm \sqrt{3}$

2.11 Galois Separability Lemma

Lemma 2.25. If α is algebraic over \mathbb{Q} then $m_\alpha(x)$ has no repeated roots in \mathbb{C} , i.e. α has exactly d conjugates in \mathbb{C} where $d = \deg(m(x)) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$

Proof. Suppose $(x - \beta)^2 \mid m_\alpha(x)$ where m_α is the minimal polynomial of β over \mathbb{Q} .

If $(x - \beta) \mid m_\alpha$ then $\alpha - \beta \mid m'_\alpha(x)$ but m'_α has smallest degree than m_α . \nmid

\square

Definition 2.26. An algebraic number field is an extension $k \supseteq \mathbb{Q}$ with $[k : \mathbb{Q}]$

By the primitive element theorem $k = \mathbb{Q}(\alpha)$ for some $\alpha \in k$ so $k \cong \mathbb{Q}[x]/(m)$ when m is the minimal polynomial of α and $\deg(m) = [k : \mathbb{Q}]$. The polynomial has exactly d roots in \mathbb{C} where $d = \deg(m)$. Call these roots α_1, α_d . Each α_i has minimal polynomial m over \mathbb{Q} .

$\therefore \mathbb{Q}[x]/(m) \cong \mathbb{Q}(\alpha_i) \subseteq \mathbb{C}$

So for each conjugate α_i of α in \mathbb{C} , there is a field homomorphism:

$$\begin{aligned} \sigma_i : k &\rightarrow \mathbb{C} \\ k &\rightarrow \mathbb{Q}[x]/(m) \rightarrow \mathbb{Q}(\alpha_i) \subseteq \mathbb{C} \end{aligned}$$

$$a_0 + a_1\alpha + \cdots + a_{d-1}\alpha \rightarrow a_0 + a_1x_1 + \cdots + a_{d-1}x^{d-1} \rightarrow a_0 + a_1\alpha_1 + \cdots + a_{d-1}\alpha_i^{d-1}$$

$$\sigma_i(a_0 + \cdots + a_{d-1}\alpha^{d-1}) = a_0 + \cdots + a_{d-1}\alpha_i^{d-1}$$

Proposition 2.27. $\sigma_1, \dots, \sigma_d$ are all the field homomorphisms from k to \mathbb{C}

E.g. $k = \mathbb{Q}(\sqrt{2})$

The conjugates of $\sqrt{2}$ in \mathbb{C} are $\pm\sqrt{2}$. $\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}$

$$\sigma_1(x + y\sqrt{2}) = x + y\sqrt{2}$$

$$\sigma_2(x + y\sqrt{2}) = x - y\sqrt{2}$$

$$k = \mathbb{Q}(\alpha), m(x) = x^3 - 2 \text{ and } \alpha_1 = 2^{\frac{1}{3}}, \alpha_2 = 2^{\frac{1}{3}}e^{\frac{2\pi i}{3}}, \alpha_3 = 2^{\frac{1}{3}}e^{\frac{4\pi i}{3}}$$