MH4920 Galois Theory & Number Fields

The Artin–Schreier theorem & Dirichlet's unit theorem

Jake Lai

21 November 2023

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Introduction

Example 1.1

The algebraic closure of $\mathbb{R}$ is $\mathbb{C}$ — $[\mathbb{C} : \mathbb{R}] = 2$.
The algebraic closure of $\mathbb{R}_{\text{alg}} := \mathbb{A} \cap \mathbb{R}$ is $\mathbb{A}$ — $[\mathbb{A} : \mathbb{R}_{\text{alg}}] = 2$.
The algebraic closure of $\mathbb{Q}$ is $\overline{\mathbb{Q}}$ — $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.
Obviously $\overline{\mathbb{C}} = \mathbb{C}$ and $\overline{\mathbb{A}} = \mathbb{A}$.

Introduction

Example 1.1

The algebraic closure of $\mathbb{R}$ is $\mathbb{C}$ — $[\mathbb{C} : \mathbb{R}] = 2$.
The algebraic closure of $\mathbb{R}_{\text{alg}} := \mathbb{A} \cap \mathbb{R}$ is $\mathbb{A}$ — $[\mathbb{A} : \mathbb{R}_{\text{alg}}] = 2$.
The algebraic closure of $\mathbb{Q}$ is $\overline{\mathbb{Q}}$ — $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.
Obviously $\overline{\mathbb{C}} = \mathbb{C}$ and $\overline{\mathbb{A}} = \mathbb{A}$.

Problem

What values can the degree of an algebraic closure take on?

The Artin–Schreier theorem

Theorem (Artin–Schreier)

Suppose F is a field not algebraically closed, and $C := \overline{F}$ is a finite extension. Then F has characteristic 0 and $C = F(i)$.

The Artin–Schreier theorem

Theorem (Artin–Schreier)

Suppose F is a field not algebraically closed, and $C := \overline{F}$ is a finite extension. Then F has characteristic 0 and $C = F(i)$.

Of course, as a corollary, $[\overline{F} : F]$ is 1, 2, or ∞.

Lemmas

Lemma 1.2

Let F be a field of characteristic $p > 0$, and $a \in F$. If $a \notin F^p$, then $x^{p^m} - a$ is irreducible in $F[x]$ for all $m \geq 1$.

Lemmas

We prove the contrapositive: if $x^{p^m} - a$ is reducible for some $m \geq 1$, then F^p contains a.

Let $x^{p^m} - a = f(x)g(x)$, where $f, g \in F[x]$ are monic. Let E be an extension of F containing a root b of of $x^{p^m} - a$, so $x^{p^m} - a = x^{p^m} - b^{p^m} = (x-b)^{p^m}$ in $E[x]$. Thus $f = (x-b)^r$ for some $0 < r < p^m$. Let $r = p^k s$. where $p \nmid s$. Then

$$f(x) = (x^{p^k} - b^{p^k})^s = x^{p^k s} - sb^{p^k} x^{p^k(s-1)} + \cdots \pm b^{p^k s},$$

so $-sb^{p^k}$ and thus b^{p^k} are in F.

Hence, $a = (b^{p^k})^{p^{m-k}} \in F^{p^{m-k}} \subset F^p$. $\square$

Lemmas

Proposition 1.3 (Artin–Schreier extensions)

Let F be a field of characteristic $p > 0$ and K/F cyclic of degree p. Then $K = F(\alpha)$, where α is a root of $x^p - x - a$ for some $a \in F$.

Lemmas

Let σ be a generator for $\mathrm{Gal}(K/F)$. Note that since $-1 \in F$ so $\sigma(-1) = -1$, we have

$$K/F(-1) = \sum_{\tau \in \mathrm{Gal}(K/F)} \tau(-1) = \sum_{k=0}^{p-1} \sigma^k(-1) = p(-1) = 0.$$

Lemmas

Let σ be a generator for $\mathrm{Gal}(K/F)$. Note that since $-1 \in F$ so $\sigma(-1) = -1$, we have

$$K/F(-1) = \sum_{\tau \in \mathrm{Gal}(K/F)} \tau(-1) = \sum_{k=0}^{p-1} \sigma^k(-1) = p(-1) = 0.$$

By the additive form of Hilbert's theorem 90, there exists $\alpha \in K$ such that $-1 = \alpha - \sigma\alpha$. Then, for $k = 0, 1, \cdots, p-1$, $\sigma^k\alpha = \alpha + k$ are the p conjugates of α in K, and thus $[F(\alpha) : F] = p$ so $K = F(\alpha)$. Since σ fixes F and

$$\sigma(\alpha^p - \alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha,$$

$\alpha^p - \alpha$ is an element of F. $\square$

Lemmas

Proposition 1.4 (Kummer extensions)

Let $n > 1$. Any cyclic extension of degree n over a field F of characteristic $q \nmid n$ containing the n^{th} roots of unity is of the form $F(\sqrt[n]{a})$ for some $a \in F$.

We omit the proof of the above, which proceeds in a similar fashion as the previous proposition.

Lemmas

Lemma 1.5

Let F be a field where -1 is not a square (so in particular $\operatorname{ch} F \neq 2$), and every element of $F(i)$ is a square. Then every finite sum of squares in F is itself a square in F, and $\operatorname{ch} F = 0$.

Lemmas

Without loss of generality, we prove the lemma for a sum of two squares. Let $a, b \in F$. There exist elements $c, d \in F$ such that $a + bi = (c + di)^2 = (c^2 - d^2) + (2cd)i$. So

$$\begin{aligned} a^2 + b^2 &= (c^2 - d^2)^2 + (2cd)^2 \\ &= c^4 - 2c^2d^2 + d^4 + 4c^2d^2 \\ &= (c^2 + d^2)^2. \end{aligned}$$

Lemmas

Without loss of generality, we prove the lemma for a sum of two squares. Let $a, b \in F$. There exist elements $c, d \in F$ such that $a + bi = (c + di)^2 = (c^2 - d^2) + (2cd)i$. So

$$\begin{aligned} a^2 + b^2 &= (c^2 - d^2)^2 + (2cd)^2 \\ &= c^4 - 2c^2d^2 + d^4 + 4c^2d^2 \\ &= (c^2 + d^2)^2. \end{aligned}$$

Suppose $\operatorname{ch} F = p > 0$. Then $-1 = \underbrace{1 + \cdots + 1}_{p-1 \text{ copies}}$, a finite sum of squares and thus itself a square; this contradicts our hypothesis. Therefore F must have characteristic 0. □

Proof of Artin–Schreier

Now we are prepared to prove the Artin–Schreier theorem.

Proof of Artin–Schreier

Now we are prepared to prove the Artin–Schreier theorem.

Theorem 1.6 (Artin–Schreier, 1926)

Let C be algebraically closed with a subfield F such that $1 < [C : F] < \infty$. Then $C = F(i)$ and $\operatorname{ch} F = 0$. Furthermore, for every nonzero $a \in F$, either a or $-a$ is a square in F, and every finite sum of squares in F is itself a square in F.

Proof of Artin–Schreier: C/F is Galois

We begin by showing that C/F is Galois. Recall the definition of Galois extensions as *normal* and *separable*. Since C is algebraically closed, it is a normal extension (every irreducible polynomial in $F[x]$ splits linearly over C).

Proof of Artin–Schreier: C/F is Galois

We begin by showing that C/F is Galois. Recall the definition of Galois extensions as *normal* and *separable*. Since C is algebraically closed, it is a normal extension (every irreducible polynomial in $F[x]$ splits linearly over C).

If $\operatorname{ch} F = 0$, F is perfect and thus C/F is automatically separable. Assume $\operatorname{ch} F = p > 0$. We claim that $F = F^p$ (i.e., the Frobenius endomorphism $a \mapsto a^p$ is an automorphism), which implies that F is perfect.

Proof of Artin–Schreier: C/F is Galois

We begin by showing that C/F is Galois. Recall the definition of Galois extensions as *normal* and *separable*. Since C is algebraically closed, it is a normal extension (every irreducible polynomial in $F[x]$ splits linearly over C).

If $\operatorname{ch} F = 0$, F is perfect and thus C/F is automatically separable. Assume $\operatorname{ch} F = p > 0$. We claim that $F = F^p$ (i.e., the Frobenius endomorphism $a \mapsto a^p$ is an automorphism), which implies that F is perfect.

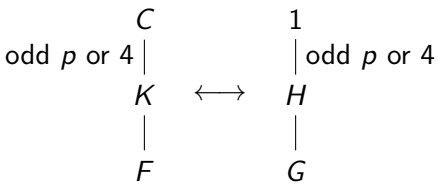
Suppose there exists an element a in F but not in F^p. Then $x^{p^m} - a$ is irreducible in $F[x]$ for all $m \geq 1$, so we may construct arbitrarily large algebraic extensions of F, contradicting the finiteness of $[C : F]$. Thus $F \subsetneq F^p \subsetneq F$.

Proof of Artin–Schreier: $[C : F]$ is never odd p or 4

Let $G = \mathrm{Gal}(C/F)$ so $[C : F] = |G|$. If $|G| > 2$, then $|G|$ is divisible by an odd prime or 4, so G contains a subgroup H of order an odd prime or 4 due to the existence of Sylow p-subgroups. By the fundamental theorem of Galois theory, C has a subfield K containing F such that $[C : K]$ is an odd prime or 4.

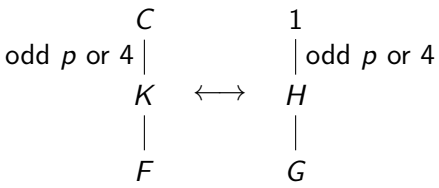
Proof of Artin–Schreier: $[C : F]$ is never odd p or 4

Let $G = \mathrm{Gal}(C/F)$ so $[C : F] = |G|$. If $|G| > 2$, then $|G|$ is divisible by an odd prime or 4, so G contains a subgroup H of order an odd prime or 4 due to the existence of Sylow p-subgroups. By the fundamental theorem of Galois theory, C has a subfield K containing F such that $[C : K]$ is an odd prime or 4.



Proof of Artin–Schreier: $[C : F]$ is never odd p or 4

Let $G = \mathrm{Gal}(C/F)$ so $[C : F] = |G|$. If $|G| > 2$, then $|G|$ is divisible by an odd prime or 4, so G contains a subgroup H of order an odd prime or 4 due to the existence of Sylow p-subgroups. By the fundamental theorem of Galois theory, C has a subfield K containing F such that $[C : K]$ is an odd prime or 4.



Thus, to prove that $[C : F] = 2$, we seek to show that $[C : F] = [C : K][K : F]$ is never divisible by an odd prime or 4. In fact, it suffices to disprove the existence of any subfield F with $[C : F]$ equals an odd prime or 4.

Proof of Artin–Schreier: C/F is not Artin–Schreier

Assume $[C : F] = p$ a prime, so that $G \cong \mathbb{Z}/p\mathbb{Z}$ is cyclic. Suppose F is of characteristic p. Then according to Artin–Schreier theory, $C = F(\alpha)$, where α is a root of some $x^p - x - a \in F[x]$. Since $\{1, \alpha, \cdots, \alpha^{p-1}\}$ is an F-basis of C, we can write any $b = b_0 + b_1\alpha + \cdots + b_{p-1}\alpha^{p-1}$, with coefficients b_j in F. Since C is algebraically closed, we can choose b such that $b^p - b = a\alpha^{p-1}$.

Proof of Artin–Schreier: C/F is not Artin–Schreier

Assume $[C : F] = p$ a prime, so that $G \cong \mathbb{Z}/p\mathbb{Z}$ is cyclic. Suppose F is of characteristic p. Then according to Artin–Schreier theory, $C = F(\alpha)$, where α is a root of some $x^p - x - a \in F[x]$. Since $\{1, \alpha, \cdots, \alpha^{p-1}\}$ is an F-basis of C, we can write any $b = b_0 + b_1\alpha + \cdots + b_{p-1}\alpha^{p-1}$, with coefficients b_j in F. Since C is algebraically closed, we can choose b such that $b^p - b = a\alpha^{p-1}$. Then

$$\begin{aligned} b^p - b &= \sum_{j=0}^{p-1} (b_j\alpha^j)^p - b_j\alpha^j \\ &= \sum_{j=0}^{p-1} b_j^p(\alpha + a)^j - b_j\alpha^j \\ &= (b_{p-1}^p - b_{p-1})\alpha^{p-1} + \cdots. \end{aligned}$$

Proof of Artin–Schreier: C/F is not Artin–Schreier

Thus $b_{p-1} \in F$ is a root of $x^p - x - a$, which is a contradiction since $x^p - x - a$ is known to be irreducible. As a consequence, F is not of characteristic $p = [C : F]$.

Assumptions:
$[C : F] = p$ prime.

Results:
ch $F \neq p$.

Proof of Artin–Schreier: C/F is not Artin–Schreier

Thus $b_{p-1} \in F$ is a root of $x^p - x - a$, which is a contradiction since $x^p - x - a$ is known to be irreducible. As a consequence, F is not of characteristic $p = [C : F]$.

Since C is algebraically closed of characteristic $\neq p$, it must contain the roots of $x^p - 1$, i.e., the p^{th} roots of unity. Because $[F(\zeta_p) : F] \leq p - 1$ and $[C : F] = p$, $[F(\zeta_p) : F]$ is forced to be 1, so $\zeta_p \in F$. By Kummer theory, $C = F(\sqrt[p]{a})$ for some $a \in F$.

Assumptions:
$[C : F] = p$ prime.

Results:
ch $F \neq p$.

Proof of Artin–Schreier: C/F is not Artin–Schreier

Thus $b_{p-1} \in F$ is a root of $x^p - x - a$, which is a contradiction since $x^p - x - a$ is known to be irreducible. As a consequence, F is not of characteristic $p = [C : F]$.

Since C is algebraically closed of characteristic $\neq p$, it must contain the roots of $x^p - 1$, i.e., the p^{th} roots of unity. Because $[F(\zeta_p) : F] \leq p - 1$ and $[C : F] = p$, $[F(\zeta_p) : F]$ is forced to be 1, so $\zeta_p \in F$. By Kummer theory, $C = F(\sqrt[p]{a})$ for some $a \in F$.

Assumptions:
$[C : F] = p$ prime.

Results:
ch $F \neq p$.
$C = F(\sqrt[p]{a})$, $a \in F$.

Proof of Artin–Schreier: Implications of C/F being Kummer

Choose $\beta \in C$ such that $\beta^p = \sqrt[p]{a}$; so $\beta^{p^2} \in F$. Let σ be a generator for $G = \mathrm{Gal}(C/F)$, so since $\beta^{p^2} = \sigma(\beta^{p^2}) = \sigma(\beta)^{p^2}$, $\sigma\beta = \omega\beta$ for some $\omega^{p^2} = 1$. We cannot have $\omega^p = 1$, since this would imply

$$\begin{aligned}\sigma(\beta^p) &= \sigma(\beta)^p \\ &= \omega^p \beta^p \\ &= \beta^p,\end{aligned}$$

or $\sqrt[p]{a} = \beta^p \in F$: a contradiction. So $\omega^p \neq 1$.

Assumptions:
$[C : F] = p$ prime.

Results:
ch $F \neq p$.
$C = F(\sqrt[p]{a})$, $a \in F$.

Proof of Artin–Schreier: Implications of C/F being Kummer

Choose $\beta \in C$ such that $\beta^p = \sqrt[p]{a}$; so $\beta^{p^2} \in F$. Let σ be a generator for $G = \mathrm{Gal}(C/F)$, so since $\beta^{p^2} = \sigma(\beta^{p^2}) = \sigma(\beta)^{p^2}$, $\sigma\beta = \omega\beta$ for some $\omega^{p^2} = 1$. We cannot have $\omega^p = 1$, since this would imply

$$\begin{aligned}\sigma(\beta^p) &= \sigma(\beta)^p \\ &= \omega^p \beta^p \\ &= \beta^p,\end{aligned}$$

or $\sqrt[p]{a} = \beta^p \in F$: a contradiction. So $\omega^p \neq 1$.

Assumptions:
$[C : F] = p$ prime.

Results:
$\mathrm{ch}\, F \neq p$.
$C = F(\sqrt[p]{a})$, $a \in F$.
$\omega^p \neq 1$.

Proof of Artin–Schreier: Implications of C/F being Kummer

ω^p is a p^{th} root of unity, and hence lies in F and is fixed by σ:

$$\omega^p = \sigma(\omega^p) = \sigma(\omega)^p,$$

therefore, $\sigma(\omega) = \zeta\omega$, where ζ is some p^{th} root of unity. Set $\zeta = \omega^{pk}$ for some integer k.

Assumptions:
$[C : F] = p$ prime.

Results:
ch $F \neq p$.
$C = F(\sqrt[p]{a})$, $a \in F$.
$\omega^p \neq 1$.

Proof of Artin–Schreier: Implications of C/F being Kummer

ω^p is a p^{th} root of unity, and hence lies in F and is fixed by σ:

$$\omega^p = \sigma(\omega^p) = \sigma(\omega)^p,$$

therefore, $\sigma(\omega) = \zeta\omega$, where ζ is some p^{th} root of unity. Set $\zeta = \omega^{pk}$ for some integer k. Thus,

$$\begin{aligned}\beta &= \sigma^p(\beta)\\ &= \sigma^{p-1}(\omega\beta)\\ &= \cdots\\ &= \omega\sigma(\omega)\cdots\sigma^{p-1}(\omega)\beta\\ &= \omega^{1+(1+pk)+\cdots+(1+pk)^{p-1}}\beta.\end{aligned}$$

Assumptions:
$[C : F] = p$ prime.

Results:
ch $F \neq p$.
$C = F(\sqrt[p]{a})$, $a \in F$.
$\omega^p \neq 1$.

Proof of Artin–Schreier: Implications of C/F being Kummer

Thus,

$$1 + (1+pk) + (1+pk)^2 + \cdots + (1+pk)^{p-1} \equiv 0 \pmod{p^2}$$
$$1 + (1+pk) + (1+2pk) + \cdots + (1+(p-1)pk) \equiv 0 \pmod{p^2}$$
$$p + \frac{p(p-1)}{2}pk \equiv 0 \pmod{p^2}$$
$$1 + \frac{p(p-1)}{2}k \equiv 0 \pmod{p}.$$

Assumptions:
$[C : F] = p$ prime.

Results:
ch $F \neq p$.
$C = F(\sqrt[p]{a})$, $a \in F$.
$\omega^p \neq 1$.

Proof of Artin–Schreier: Implications of C/F being Kummer

Thus,

$$1 + (1 + pk) + (1 + pk)^2 + \cdots + (1 + pk)^{p-1} \equiv 0 \pmod{p^2}$$
$$1 + (1 + pk) + (1 + 2pk) + \cdots + (1 + (p-1)pk) \equiv 0 \pmod{p^2}$$
$$p + \frac{p(p-1)}{2} pk \equiv 0 \pmod{p^2}$$
$$1 + \frac{p(p-1)}{2} k \equiv 0 \pmod{p}.$$

The last congruence can be satisfied only if $p = 2$. In fact, it can be shown that $\omega^2 = -1$ so that $C = F(i)$.

Assumptions:
$[C : F] = p$ prime.

Results:
ch $F \neq p$.
$C = F(\sqrt[p]{a})$, $a \in F$.
$\omega^p \neq 1$.

Proof of Artin–Schreier: Implications of C/F being Kummer

Thus,

$$1 + (1+pk) + (1+pk)^2 + \cdots + (1+pk)^{p-1} \equiv 0 \pmod{p^2}$$
$$1 + (1+pk) + (1+2pk) + \cdots + (1+(p-1)pk) \equiv 0 \pmod{p^2}$$
$$p + \frac{p(p-1)}{2}pk \equiv 0 \pmod{p^2}$$
$$1 + \frac{p(p-1)}{2}k \equiv 0 \pmod{p}.$$

The last congruence can be satisfied only if $p = 2$. In fact, it can be shown that $\omega^2 = -1$ so that $C = F(i)$.

Results:
If $[C : F]$ is prime, $C = F(i)$ with $\operatorname{ch} F \neq 2$.

Proof of Artin–Schreier: $[C : F] \neq 4$

Finally, suppose $[C : F] = 4$. Since $\mathrm{Gal}(C/F)$ then has a subgroup of order 2, there must be an intermediate field $F \subset K \subset C$ with $[C : K] = 2$. We just showed that i cannot be in any such field K with $[C : K] = 2$, but

$$[C : F(i)] = [C : F]/[F(i) : F] = 4/2 = 2$$

and clearly $i \in F(i)$; a contradiction.

Results:
If $[C : F]$ is prime, $C = F(i)$ with $\mathrm{ch}\, F \neq 2$.

Proof of Artin–Schreier: $[C : F] \neq 4$

Finally, suppose $[C : F] = 4$. Since $\mathrm{Gal}(C/F)$ then has a subgroup of order 2, there must be an intermediate field $F \subset K \subset C$ with $[C : K] = 2$. We just showed that i cannot be in any such field K with $[C : K] = 2$, but

$$[C : F(i)] = [C : F]/[F(i) : F] = 4/2 = 2$$

and clearly $i \in F(i)$; a contradiction.

Thus, $[C : F] \neq 4$, so the only possibility is that $[C : F] = 2$. All that remains is to show that F has characteristic 0.

Results:
If $[C : F]$ is prime, $C = F(i)$ with $\mathrm{ch}\, F \neq 2$.

Proof of Artin–Schreier: ch $F = 0$

Suppose a and $-a$ are both not squares in F. Then $C = F(\sqrt{a}) = F(\sqrt{-a})$. Since $\frac{\sqrt{-a}}{\sqrt{a}} = \frac{(\sqrt{a})(\sqrt{-a})}{a} \in F$ (the product of roots is the constant coefficient, hence in F), $\frac{-a}{a} = -1$ is a square in F, which contradicts $i \notin F$. Thus, exactly one of a and $-a$ is a square in F.

Proof of Artin–Schreier: ch $F = 0$

Suppose a and $-a$ are both not squares in F. Then $C = F(\sqrt{a}) = F(\sqrt{-a})$. Since $\frac{\sqrt{-a}}{\sqrt{a}} = \frac{(\sqrt{a})(\sqrt{-a})}{a} \in F$ (the product of roots is the constant coefficient, hence in F), $\frac{-a}{a} = -1$ is a square in F, which contradicts $i \notin F$. Thus, exactly one of a and $-a$ is a square in F.

Noticing that all hypotheses are satisfied, we may apply Lemma 1.5 to conclude the proof. □

Some remarks

Such fields F are called *real closed fields*, and there is a notion of the *real closure* of an ordered field. Such fields were also studied as part of mathematical logic (model theory) by Tarski in the 1930s.

Some remarks

Such fields F are called *real closed fields*, and there is a notion of the *real closure* of an ordered field. Such fields were also studied as part of mathematical logic (model theory) by Tarski in the 1930s.

Using Artin–Schreier theory, Artin (1927) also resolved Hilbert's 17^{th} problem affirmatively: every positive semi-definite polynomial $f \in F[x]$ over a real closed field F can be represented as the sum of squares of rational functions $r_i \in F(x)$.

Some remarks

Such fields F are called *real closed fields*, and there is a notion of the *real closure* of an ordered field. Such fields were also studied as part of mathematical logic (model theory) by Tarski in the 1930s.

Using Artin–Schreier theory, Artin (1927) also resolved Hilbert's 17^{th} problem affirmatively: every positive semi-definite polynomial $f \in F[x]$ over a real closed field F can be represented as the sum of squares of rational functions $r_i \in F(x)$.

We proved the basic results of Kummer theory and Artin–Schreier theory using Hilbert's theorem 90, which rested on the linear independence of characters. But Theorem 90 can also be recast more generally for non-cyclic extensions in terms of *Galois cohomology*, the (co)homology of modules acted on by a Galois group. Galois cohomology appears elsewhere: e.g., underlying the arithmetic of elliptic curves, in local class field theory (my next stop, I think).

Disclaimer

(This section was created post hoc! The second half of the original presentation was conducted using the whiteboard. The notes are available at https://jakelai.me/gtnfnotes.pdf.)

Dirichlet's unit theorem

Let K be a number field of degree n over $\mathbb{Q}$, with r_1 real and $2r_2$ nonreal embeddings.

Dirichlet's unit theorem

Let K be a number field of degree n over $\mathbb{Q}$, with r_1 real and $2r_2$ nonreal embeddings.

Theorem (Dirichlet's unit)

The unit group of a number ring $\mathcal{O}_K$ is of the form $\mathcal{O}_K^\times \cong \mu(\mathcal{O}_K) \times W$, where W is a free abelian group of rank $r_1 + r_2 - 1$. (Every unit is of the form $\zeta \varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}$ — the ε_i are multiplicatively independent, *together a* fundamental system of units.*)*

Dirichlet's unit theorem

Let K be a number field of degree n over $\mathbb{Q}$, with r_1 real and $2r_2$ nonreal embeddings.

Theorem (Dirichlet's unit)

The unit group of a number ring $\mathcal{O}_K$ is of the form $\mathcal{O}_K^\times \cong \mu(\mathcal{O}_K) \times W$, where W is a free abelian group of rank $r_1 + r_2 - 1$. (Every unit is of the form $\zeta \varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}$ — the ε_i are multiplicatively independent, *together a* fundamental system of units.*)*

We use Minkowski's *geometry of numbers*.

Proof of the unit theorem: G/U is compact

Embed $\mathcal{O}_K$ in $V := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as a lattice $\wedge$, and $\mathcal{O}_K^\times$ as $U \leq G := \{v \in V : |\mathrm{N}(v)| = 1\}$.

Proof of the unit theorem: G/U is compact

Embed $\mathcal{O}_K$ in $V := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as a lattice $\wedge$, and $\mathcal{O}_K^\times$ as $U \leq G := \{v \in V : |\mathrm{N}(v)| = 1\}$.

Lemma 2.1

For each positive integer N, only finitely many $a \in \mathcal{O}_K$ satisfy $|\mathrm{N}_{\mathbb{Q}}^K(a)| = N$ (up to multiplication by a unit).

Proof of the unit theorem: G/U is compact

Embed $\mathcal{O}_K$ in $V := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as a lattice $\wedge$, and $\mathcal{O}_K^\times$ as $U \leq G := \{v \in V : |\mathrm{N}(v)| = 1\}$.

Lemma 2.1

For each positive integer N, only finitely many $a \in \mathcal{O}_K$ satisfy $|\mathrm{N}_{\mathbb{Q}}^K(a)| = N$ (up to multiplication by a unit).

By Minkowski's theorem, for any $g \in G$ there exists a compact, centrally symmetric convex body $g^{-1}C \subset V$ such that there is some nonzero $a \in g^{-1}C \cap (\wedge - \{0\})$.
$|\mathrm{N}_{\mathbb{Q}}^K(a)| = |\mathrm{N}(a)| \in |\mathrm{N}(g^{-1}C)| = |\mathrm{N}(C)|$ (bounded set since C is compact).
$\mathrm{N}_{\mathbb{Q}}^K(a) \in \mathbb{Z}$, so there must be finitely many values $N = |\mathrm{N}_{\mathbb{Q}}^K(a)|$ (a bounded set of integers is finite).

Proof of the unit theorem: G/U is compact

Thus there are finitely many a_i such that $a_i U$ has a point lying in $g^{-1}C$. 'Multiply' this picture by ga_i^{-1}: every coset gU has a representative lying in some $a_i^{-1}C$.

Proof of the unit theorem: G/U is compact

Thus there are finitely many a_i such that $a_i U$ has a point lying in $g^{-1}C$. 'Multiply' this picture by ga_i^{-1}: every coset gU has a representative lying in some $a_i^{-1}C$.

$G \cup \bigcap_i a_i^{-1}C$ is the intersection of closed G and a finite union of compact sets, itself compact; it contains all coset representatives of G/U, so there is a surjection onto G/U. Thus,

Theorem

G/U is compact.

Proof of the unit theorem: structure of $\ker L|_U$

The *logarithmic mapping* $L : V \to \mathbb{R}^{r_1+r_2}$ takes $(\cdots, x_i, \cdots, z_j \cdots)$ to $(\cdots, \log|x_i|, \cdots, 2\log|z_j|, \cdots)$ and maps G to the hyperplane $\{(y_i) : \sum_i y_i = 0\}$ of dimension $r_1 + r_2 - 1$.

Proof of the unit theorem: structure of $\ker L|_U$

The *logarithmic mapping* $L : V \to \mathbb{R}^{r_1+r_2}$ takes $(\cdots, x_i, \cdots, z_j \cdots)$ to $(\cdots, \log|x_i|, \cdots, 2\log|z_j|, \cdots)$ and maps G to the hyperplane $\{(y_i) : \sum_i y_i = 0\}$ of dimension $r_1 + r_2 - 1$.

The kernel of L restricted to U is compact and discrete, hence finite, so must be comprised of roots of unity of U. But all roots of unity of U are in $\ker L|_U$. Hence the kernel of $L|_U$ is precisely $\mu(\mathcal{O}_K)$.

Proof of the unit theorem: structure of $\ker L|_U$

The *logarithmic mapping* $L : V \to \mathbb{R}^{r_1+r_2}$ takes $(\cdots, x_i, \cdots, z_j \cdots)$ to $(\cdots, \log|x_i|, \cdots, 2\log|z_j|, \cdots)$ and maps G to the hyperplane $\{(y_i) : \sum_i y_i = 0\}$ of dimension $r_1 + r_2 - 1$.

The kernel of L restricted to U is compact and discrete, hence finite, so must be comprised of roots of unity of U. But all roots of unity of U are in $\ker L|_U$. Hence the kernel of $L|_U$ is precisely $\mu(\mathcal{O}_K)$.

Proof of the unit theorem: structure of $L(U)$

L is a continuous surjective group homomorphism, so the induced map $G/U \to L(G)/L(U)$ is also surjective. Thus, $L(G)/L(U)$ is compact. But the only way the quotient of $\mathbb{R}^r$ modulo a discrete subgroup is compact is the subgroup has rank r. (Consider the noncompact cylinder $\mathbb{R}^2/\mathbb{Z}$ vs. the compact torus $\mathbb{R}^2/\mathbb{Z}^2$.)

Proof of the unit theorem: structure of $L(U)$

L is a continuous surjective group homomorphism, so the induced map $G/U \to L(G)/L(U)$ is also surjective. Thus, $L(G)/L(U)$ is compact. But the only way the quotient of $\mathbb{R}^r$ modulo a discrete subgroup is compact is the subgroup has rank r. (Consider the noncompact cylinder $\mathbb{R}^2/\mathbb{Z}$ vs. the compact torus $\mathbb{R}^2/\mathbb{Z}^2$.)

Therefore, since $L(G) \cong \mathbb{R}^{r_1+r_2-1}$, $L(U) \cong \mathbb{Z}^{r_1+r_2-1}$.

Proof of the unit theorem: structure of $L(U)$

L is a continuous surjective group homomorphism, so the induced map $G/U \to L(G)/L(U)$ is also surjective. Thus, $L(G)/L(U)$ is compact. But the only way the quotient of $\mathbb{R}^r$ modulo a discrete subgroup is compact is the subgroup has rank r. (Consider the noncompact cylinder $\mathbb{R}^2/\mathbb{Z}$ vs. the compact torus $\mathbb{R}^2/\mathbb{Z}^2$.)

Therefore, since $L(G) \cong \mathbb{R}^{r_1+r_2-1}$, $L(U) \cong \mathbb{Z}^{r_1+r_2-1}$. By the fundamental homomorphism theorem:

$$U \cong \mu(\mathcal{O}_K) \times \mathbb{Z}^{r_1+r_2-1}.$$

The multiplicative independence of the ε_i's follows from the $\mathbb{Z}$-linear independence of their images under L. $\square$

Applications

Theorem (Artin)

Let $\mathcal{O}_K$ be the number ring of a cubic field K with $r_1 = 1, r_2 = 1$, so $\mathcal{O}_K^\times$ has rank $1 + 1 - 1 = 1$. Viewing K in $\mathbb{R}$, if $u > 1$ is a unit of $\mathcal{O}_K$, then $4u^3 + 24 > |\operatorname{disc} \mathcal{O}_K|$.

Applications

Theorem (Artin)

Let $\mathcal{O}_K$ be the number ring of a cubic field K with $r_1 = 1, r_2 = 1$, so $\mathcal{O}_K^\times$ has rank $1 + 1 - 1 = 1$. Viewing K in $\mathbb{R}$, if $u > 1$ is a unit of $\mathcal{O}_K$, then $4u^3 + 24 > |\operatorname{disc} \mathcal{O}_K|$.

As a collorary, if $4u^{3/2} + 24 \leq |\operatorname{disc} \mathcal{O}_K|$, then $u = \varepsilon$ the fundamental unit of $\mathcal{O}_K$. In $\mathbb{Q}(\sqrt[3]{2})$, $\operatorname{disc} \mathcal{O}_K = -108$. $u = 1 + \sqrt[3]{2} + \sqrt[3]{4} \approx 3.847$ satisfies $4u^{3/2} + 24 \approx 54.185 \leq 108$, so u is the fundamental unit.

Applications

Let $r = r_1 + r_2 - 1$, and $u_1, \cdots, u_r$ be units in K. Consider the $r \times (r+1)$ matrix

$$M = \begin{pmatrix} \log|\sigma_1(u_1)| & \cdots & 2\log|\tau_{r_2}(u_1)| \\ \vdots & \ddots & \vdots \\ \log|\sigma_1(u_1)| & \cdots & 2\log|\tau_{r_2}(u_r)| \end{pmatrix}$$

Each row of M sums to 0; removing any column does not change the determinant of the resulting matrix M'.

Applications

Let $r = r_1 + r_2 - 1$, and $u_1, \cdots, u_r$ be units in K. Consider the $r \times (r+1)$ matrix

$$M = \begin{pmatrix} \log|\sigma_1(u_1)| & \cdots & 2\log|\tau_{r_2}(u_1)| \\ \vdots & \ddots & \vdots \\ \log|\sigma_1(u_1)| & \cdots & 2\log|\tau_{r_2}(u_r)| \end{pmatrix}$$

Each row of M sums to 0; removing any column does not change the determinant of the resulting matrix M'.

The *regulator* $\operatorname{reg}(u_1, \cdots, u_r) := |\det M'|$. The regulator of a number ring $\operatorname{reg} \mathcal{O}_K$ is the regulator of its fundamental units. In a way, the regulator measures the 'density' of the units.

Applications

The regulator also appears in the remarkable *class number formula*:

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\cdot \operatorname{reg}\mathcal{O}_K \cdot h}{|\mu(\mathcal{O}_K)|\sqrt{|\operatorname{disc}\mathcal{O}_K|}},$$

where h is the *class number*, or size of the ideal class group.

Applications

The regulator also appears in the remarkable *class number formula*:

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\cdot \operatorname{reg}\mathcal{O}_K \cdot h}{|\mu(\mathcal{O}_K)|\sqrt{|\operatorname{disc}\mathcal{O}_K|}},$$

where h is the *class number*, or size of the ideal class group.

Generalisations of the regulator (*higher regulators*) are involved in results and conjectures on special values of L-functions: Birch–Swinnerton-Dyer, Stark, Beilinson.

Applications

The regulator also appears in the remarkable *class number formula*:

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\cdot \operatorname{reg}\mathcal{O}_K \cdot h}{|\mu(\mathcal{O}_K)|\sqrt{|\operatorname{disc}\mathcal{O}_K|}},$$

where h is the *class number*, or size of the ideal class group.

Generalisations of the regulator (*higher regulators*) are involved in results and conjectures on special values of L-functions: Birch–Swinnerton-Dyer, Stark, Beilinson.

'In my opinion, conjectures about special points and special values of L-functions are the most beautiful in all of mathematics.'

— Henri Cohen, *Number Theory, Volume II: Analytic and Modern Tools*.

Thank you!

Bibliography I

[1] Keith Conrad. "Dirichlet's unit theorem". In: *Self-published* (). URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/unittheorem.pdf.

[2] Keith Conrad. "Linear independence of characters". In: *Self-published* (2008). URL: http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/linearchar.pdf.

[3] Keith Conrad. "The Artin-Schreier theorem". In: *Self-published* (2011). URL: http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/artinschreier.pdf.

[4] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, 2003. 944 pp. ISBN: 978-0-471-43334-7.

[5] Nathan Jacobson. *Basic Algebra II*. Courier Corporation, 2009. 704 pp. ISBN: 978-0-486-47187-7.

Bibliography II

[6] Daniel A. Marcus. *Number Fields*. Universitext. Springer International Publishing, 2018. 203 pp. ISBN: 978-3-319-90233-3.