Math 361

April 17, 2023

Projects

Monday

Bram: RSA encryption using lattices associated with number fields

Callie: Totally real fields

Wednesday

Richard: $ax^2 + by^2 = cz^2$

Zack: Two proofs of the sum of two squares theorem

Friday

Kellen: Polynomial factorization

Patrick: The Pell equation

Projects: initial meetings

Wednesday

Bram:	1:40–2:05
Richard	2:05–2:30
Callie	2:30–2:55

Friday

Patrick	1:40–2:05
Zack	2:05–2:30
Kellen	2:30–2:55

For the meeting: Create a slide with a draft outline of your presentation.

There is a template beamer file at the bottom of our course homepage.

Projects: preparation

Most important point:

Practice your presentation several times with a stopwatch.

Today

Dirichlet's unit theorem.

Units in a number field

Let K be a number field, and let $\mathfrak{O}_K^*$ denote the units in $\mathfrak{O}_K$.

Units in a number field

Let K be a number field, and let $\mathfrak{O}_K^*$ denote the units in $\mathfrak{O}_K$.

Example.

- We have $\pm 1 \in \mathfrak{O}_K^*$ for all K.

Units in a number field

Let K be a number field, and let $\mathfrak{O}_K^*$ denote the units in $\mathfrak{O}_K$.

Example.

- We have $\pm 1 \in \mathfrak{O}_K^*$ for all K.
- If $K = \mathbb{Q}(i)$, then $\mathfrak{O}_K^* = \{\pm 1, \pm i\}$.

Units in a number field

Let K be a number field, and let $\mathfrak{O}_K^*$ denote the units in $\mathfrak{O}_K$.

Example.

- We have $\pm 1 \in \mathfrak{O}_K^*$ for all K.
- If $K = \mathbb{Q}(i)$, then $\mathfrak{O}_K^* = \{\pm 1, \pm i\}$.
- If $K = \mathbb{Q}(\sqrt{2})$, then $1 + \sqrt{2} \in \mathfrak{O}_K^*$.

Units in a number field

Let K be a number field, and let $\mathfrak{O}_K^*$ denote the units in $\mathfrak{O}_K$.

Example.

- We have $\pm 1 \in \mathfrak{O}_K^*$ for all K.
- If $K = \mathbb{Q}(i)$, then $\mathfrak{O}_K^* = \{\pm 1, \pm i\}$.
- If $K = \mathbb{Q}(\sqrt{2})$, then $1 + \sqrt{2} \in \mathfrak{O}_K^*$. Since $|1 + \sqrt{2}| > 1$, we see $\{(1 + \sqrt{2})^k : k \in \mathbb{Z}_{>0}\}$ is an infinite collection of units in $\mathfrak{O}_K^*$.

Units in a number field

Let K be a number field, and let $\mathfrak{O}_K^*$ denote the units in $\mathfrak{O}_K$.

Example.

- We have $\pm 1 \in \mathfrak{O}_K^*$ for all K.
- If $K = \mathbb{Q}(i)$, then $\mathfrak{O}_K^* = \{\pm 1, \pm i\}$.
- If $K = \mathbb{Q}(\sqrt{2})$, then $1 + \sqrt{2} \in \mathfrak{O}_K^*$. Since $|1 + \sqrt{2}| > 1$, we see $\{(1 + \sqrt{2})^k : k \in \mathbb{Z}_{>0}\}$ is an infinite collection of units in $\mathfrak{O}_K^*$.

  So the group of units in $\mathbb{Q}(\sqrt{2})$ is at least as large as

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$.
(Reminder of proof on blackboard.)

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$. (Reminder of proof on blackboard.)

(c) Elements of finite order in $\mathfrak{O}_K^*$ are roots of unity, and every root of unity in K is in $\mathfrak{O}_K^*$.

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$. (Reminder of proof on blackboard.)

(c) Elements of finite order in $\mathfrak{O}_K^*$ are roots of unity, and every root of unity in K is in $\mathfrak{O}_K^*$. (If $\zeta \in K$ and $\zeta^m = 1$, them ζ satisfies $x^m - 1$, and hence is an algebraic integer in K.)

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$. (Reminder of proof on blackboard.)

(c) Elements of finite order in $\mathfrak{O}_K^*$ are roots of unity, and every root of unity in K is in $\mathfrak{O}_K^*$. (If $\zeta \in K$ and $\zeta^m = 1$, them ζ satisfies $x^m - 1$, and hence is an algebraic integer in K.)

(d) The elements of $\mathfrak{O}_K$ with finite order form a finite cyclic subgroup of $\mathfrak{O}_K$ of even order.

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$. (Reminder of proof on blackboard.)

(c) Elements of finite order in $\mathfrak{O}_K^*$ are roots of unity, and every root of unity in K is in $\mathfrak{O}_K^*$. (If $\zeta \in K$ and $\zeta^m = 1$, them ζ satisfies $x^m - 1$, and hence is an algebraic integer in K.)

(d) The elements of $\mathfrak{O}_K$ with finite order form a finite cyclic subgroup of $\mathfrak{O}_K$ of even order.

Proof. These elements clearly form a subgroup.

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$. (Reminder of proof on blackboard.)

(c) Elements of finite order in $\mathfrak{O}_K^*$ are roots of unity, and every root of unity in K is in $\mathfrak{O}_K^*$. (If $\zeta \in K$ and $\zeta^m = 1$, them ζ satisfies $x^m - 1$, and hence is an algebraic integer in K.)

(d) The elements of $\mathfrak{O}_K$ with finite order form a finite cyclic subgroup of $\mathfrak{O}_K$ of even order.

Proof. These elements clearly form a subgroup. For finiteness, note that the mapping $\sigma : K \to \mathbb{L}^{s,t} \simeq \mathbb{R}^n$ maps $\mathfrak{O}_K$ to a lattice in $\mathbb{R}^n$, and the image of $\{\zeta \in K : |\zeta| = 1\}$ maps to a compact set.

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$. (Reminder of proof on blackboard.)

(c) Elements of finite order in $\mathfrak{O}_K^*$ are roots of unity, and every root of unity in K is in $\mathfrak{O}_K^*$. (If $\zeta \in K$ and $\zeta^m = 1$, them ζ satisfies $x^m - 1$, and hence is an algebraic integer in K.)

(d) The elements of $\mathfrak{O}_K$ with finite order form a finite cyclic subgroup of $\mathfrak{O}_K$ of even order.

Proof. These elements clearly form a subgroup. For finiteness, note that the mapping $\sigma : K \to \mathbb{L}^{s,t} \simeq \mathbb{R}^n$ maps $\mathfrak{O}_K$ to a lattice in $\mathbb{R}^n$, and the image of $\{\zeta \in K : |\zeta| = 1\}$ maps to a compact set. Since $-1 \in \mathfrak{O}_K$ and has order 2, it follows that 2 divides the order of the subgroup.

First properties

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$. (Reminder of proof on blackboard.)

(c) Elements of finite order in $\mathfrak{O}_K^*$ are roots of unity, and every root of unity in K is in $\mathfrak{O}_K^*$. (If $\zeta \in K$ and $\zeta^m = 1$, them ζ satisfies $x^m - 1$, and hence is an algebraic integer in K.)

(d) The elements of $\mathfrak{O}_K$ with finite order form a finite cyclic subgroup of $\mathfrak{O}_K$ of even order.

Proof. These elements clearly form a subgroup. For finiteness, note that the mapping $\sigma : K \to \mathbb{L}^{s,t} \simeq \mathbb{R}^n$ maps $\mathfrak{O}_K$ to a lattice in $\mathbb{R}^n$, and the image of $\{\zeta \in K : |\zeta| = 1\}$ maps to a compact set. Since $-1 \in \mathfrak{O}_K$ and has order 2, it follows that 2 divides the order of the subgroup. A finite subgroup of K^* must be cyclic (see the notes for Friday, Week 10). $\square$

Dirichlet's unit theorem

Theorem. Let K have s real embeddings and $2t$ complex embeddings.

Dirichlet's unit theorem

Theorem. Let K have s real embeddings and $2t$ complex embeddings. Then, we have a group isomorphism

$$\mathfrak{O}_K^* \simeq W \times \mathbb{Z}^{s+t-1}$$

where W is the finite cyclic group of roots of unity in K (the subgroup of $\mathfrak{O}_K$ of elements of finite order).

Dirichlet's unit theorem

Theorem. Let K have s real embeddings and $2t$ complex embeddings. Then, we have a group isomorphism

$$\mathfrak{O}_K^* \simeq W \times \mathbb{Z}^{s+t-1}$$

where W is the finite cyclic group of roots of unity in K (the subgroup of $\mathfrak{O}_K$ of elements of finite order).

Proof. See our textbook, Appendix B.

Dirichlet's unit theorem: ideal of proof

Consider the mapping

Dirichlet's unit theorem: ideal of proof

Consider the mapping

$$\ell\colon \mathfrak{O}_K^* \xrightarrow{\sigma} \mathbb{R}^s \times \mathbb{C}^t \to \mathbb{R}^{s+t}$$

$$(x_1, \ldots, x_s, z_1, \ldots, z_t) \mapsto (\ln|x_1|, \ldots, \ln|x_s|, \ln|z_1|^2, \ldots, \ln|z_t|^2).$$

Dirichlet's unit theorem: ideal of proof

Consider the mapping

$$\ell\colon \mathfrak{O}_K^* \xrightarrow{\sigma} \mathbb{R}^s \times \mathbb{C}^t \to \mathbb{R}^{s+t}$$

$$(x_1, \ldots, x_s, z_1, \ldots, z_t) \mapsto (\ln|x_1|, \ldots, \ln|x_s|, \ln|z_1|^2, \ldots, \ln|z_t|^2).$$

ℓ takes a multiplicative group to an additive subgroup of $\mathbb{R}^{s+t}$.

Dirichlet's unit theorem: ideal of proof

Consider the mapping

$$\ell\colon \mathfrak{O}_K^* \xrightarrow{\sigma} \mathbb{R}^s \times \mathbb{C}^t \to \mathbb{R}^{s+t}$$

$$(x_1, \ldots, x_s, z_1, \ldots, z_t) \mapsto (\ln|x_1|, \ldots, \ln|x_s|, \ln|z_1|^2, \ldots, \ln|z_t|^2).$$

ℓ takes a multiplicative group to an additive subgroup of $\mathbb{R}^{s+t}$.

It turns out that the image of ℓ is a lattice of rank $s + t - 1$,

Dirichlet's unit theorem: ideal of proof

Consider the mapping

$$\ell\colon \mathfrak{O}_K^* \xrightarrow{\sigma} \mathbb{R}^s \times \mathbb{C}^t \to \mathbb{R}^{s+t}$$

$$(x_1, \ldots, x_s, z_1, \ldots, z_t) \mapsto (\ln|x_1|, \ldots, \ln|x_s|, \ln|z_1|^2, \ldots, \ln|z_t|^2).$$

ℓ takes a multiplicative group to an additive subgroup of $\mathbb{R}^{s+t}$.

It turns out that the image of ℓ is a lattice of rank $s+t-1$, and that $\ker(\ell) = W$, the roots of unity in K.

Dirichlet's unit theorem: ideal of proof

Consider the mapping

$$\ell\colon \mathfrak{O}_K^* \xrightarrow{\sigma} \mathbb{R}^s \times \mathbb{C}^t \to \mathbb{R}^{s+t}$$

$$(x_1, \ldots, x_s, z_1, \ldots, z_t) \mapsto (\ln|x_1|, \ldots, \ln|x_s|, \ln|z_1|^2, \ldots, \ln|z_t|^2).$$

ℓ takes a multiplicative group to an additive subgroup of $\mathbb{R}^{s+t}$.

It turns out that the image of ℓ is a lattice of rank $s+t-1$, and that $\ker(\ell) = W$, the roots of unity in K. The result follows.

Dirichlet's unit theorem: ideal of proof

Consider the mapping

$$\ell\colon \mathfrak{O}_K^* \xrightarrow{\sigma} \mathbb{R}^s \times \mathbb{C}^t \to \mathbb{R}^{s+t}$$

$$(x_1, \ldots, x_s, z_1, \ldots, z_t) \mapsto (\ln|x_1|, \ldots, \ln|x_s|, \ln|z_1|^2, \ldots, \ln|z_t|^2).$$

ℓ takes a multiplicative group to an additive subgroup of $\mathbb{R}^{s+t}$.

It turns out that the image of ℓ is a lattice of rank $s+t-1$, and that $\ker(\ell) = W$, the roots of unity in K. The result follows.

On the blackboard: It's easy to show $W \subseteq \ker(\ell)$,

Dirichlet's unit theorem: ideal of proof

Consider the mapping

$$\ell\colon \mathfrak{O}_K^* \xrightarrow{\sigma} \mathbb{R}^s \times \mathbb{C}^t \to \mathbb{R}^{s+t}$$

$$(x_1, \ldots, x_s, z_1, \ldots, z_t) \mapsto (\ln|x_1|, \ldots, \ln|x_s|, \ln|z_1|^2, \ldots, \ln|z_t|^2).$$

ℓ takes a multiplicative group to an additive subgroup of $\mathbb{R}^{s+t}$.

It turns out that the image of ℓ is a lattice of rank $s+t-1$, and that $\ker(\ell) = W$, the roots of unity in K. The result follows.

On the blackboard: It's easy to show $W \subseteq \ker(\ell)$, and that the image of ℓ has rank at most $s+t-1$.

Examples

W is the finite cyclic group of roots of unity in K.

Examples

W is the finite cyclic group of roots of unity in K.

The only roots of unity that are real are ± 1.

Examples

W is the finite cyclic group of roots of unity in K.

The only roots of unity that are real are ± 1.

A field embedding preserves roots of unity and their orders.

Examples

W is the finite cyclic group of roots of unity in K.

The only roots of unity that are real are ± 1.

A field embedding preserves roots of unity and their orders.

Therefore, if K has any real embedding, $W = \{-1, 1\}$.

Examples

W is the finite cyclic group of roots of unity in K.

The only roots of unity that are real are ± 1.

A field embedding preserves roots of unity and their orders.

Therefore, if K has any real embedding, $W = \{-1, 1\}$.

Question: For arbitrary K, when is the group of units finite?

Example

Consider $K = \mathbb{Q}(\sqrt{2})$. Since K is real, $W = \{-1, 1\}$.

Example

Consider $K = \mathbb{Q}(\sqrt{2})$. Since K is real, $W = \{-1, 1\}$.

We have $s = 2$ and $t = 1$. Therefore, the unit group in K has the form

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Example

Consider $K = \mathbb{Q}(\sqrt{2})$. Since K is real, $W = \{-1, 1\}$.

We have $s = 2$ and $t = 1$. Therefore, the unit group in K has the form

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

We have seen that $1 + \sqrt{2}$ is a unit of infinite order.

Example

Consider $K = \mathbb{Q}(\sqrt{2})$. Since K is real, $W = \{-1, 1\}$.

We have $s = 2$ and $t = 1$. Therefore, the unit group in K has the form

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

We have seen that $1 + \sqrt{2}$ is a unit of infinite order. However, we did not prove it corresponds to a generator the factor of $\mathbb{Z}$.

Example

Consider $K = \mathbb{Q}(\sqrt{2})$. Since K is real, $W = \{-1, 1\}$.

We have $s = 2$ and $t = 1$. Therefore, the unit group in K has the form

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

We have seen that $1 + \sqrt{2}$ is a unit of infinite order. However, we did not prove it corresponds to a generator the factor of $\mathbb{Z}$.

In other words, we have not shown that the full set of units in $\mathfrak{O}_K$ is $\pm(1 + \sqrt{2})$.