On Number Fields with Unit Group of a Prescribed Reduction

Kyle Wu
Mentor: Dr. Alexander Petrov

MIT Primes Conference, October 18-19

Fields

A field $(F, +, \cdot)$ is a commutative ring with multiplicative identity such that every non-zero element is invertible.

Fields

A field $(F, +, \cdot)$ is a commutative ring with multiplicative identity such that every non-zero element is invertible.

Example

We have that $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ are fields under the standard operations and $\mathbb{F}_7$ (residues modulo 7) is a field under operations modulo 7.

Number Fields

A number field K is a field extension of $\mathbb{Q}$ of finite degree.

Number Fields

A number field K is a field extension of $\mathbb{Q}$ of finite degree.

An algebraic number is a root of an integer polynomial. An algebraic integer is a root of a monic integer polynomial.

Number Fields

A number field K is a field extension of $\mathbb{Q}$ of finite degree.

An algebraic number is a root of an integer polynomial. An algebraic integer is a root of a monic integer polynomial.

- Number fields are very closely related to algebraic numbers.
- Any number field K can be written in the form $\mathbb{Q}(\alpha)$, or $\mathbb{Q}$ with α adjoined for some algebraic integer α.
- The degree of K is then equal to the degree of the minimal polynomial of α.

Number Fields

A number field K is a field extension of $\mathbb{Q}$ of finite degree.

An algebraic number is a root of an integer polynomial. An algebraic integer is a root of a monic integer polynomial.

- Number fields are very closely related to algebraic numbers.
- Any number field K can be written in the form $\mathbb{Q}(\alpha)$, or $\mathbb{Q}$ with α adjoined for some algebraic integer α.
- The degree of K is then equal to the degree of the minimal polynomial of α.

Example

As from before, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a number field of degree 2.

Ring of Integers and Unit Group

The ring of integers $\mathcal{O}_K$ of a number field K is the ring of all algebraic integers contained in K.

Ring of Integers and Unit Group

The ring of integers $\mathcal{O}_K$ of a number field K is the ring of all algebraic integers contained in K.

Example

The ring of integers of $\mathbb{Q}(\sqrt{2})$ is equal to $\mathbb{Z}[\sqrt{2}]$.

Ring of Integers and Unit Group

The ring of integers $\mathcal{O}_K$ of a number field K is the ring of all algebraic integers contained in K.

Example

The ring of integers of $\mathbb{Q}(\sqrt{2})$ is equal to $\mathbb{Z}[\sqrt{2}]$.

The unit group $\mathcal{O}_K^\times$ of the ring of integers is the multiplicative group of elements of $\mathcal{O}_K$ whose inverses lie in $\mathcal{O}_K$.

Ring of Integers and Unit Group

The ring of integers $\mathcal{O}_K$ of a number field K is the ring of all algebraic integers contained in K.

Example

The ring of integers of $\mathbb{Q}(\sqrt{2})$ is equal to $\mathbb{Z}[\sqrt{2}]$.

The unit group $\mathcal{O}_K^\times$ of the ring of integers is the multiplicative group of elements of $\mathcal{O}_K$ whose inverses lie in $\mathcal{O}_K$.

Example

The unit group of $\mathbb{Z}[\sqrt{2}]$ is $\pm(1+\sqrt{2})^{\mathbb{Z}} = \{\pm(1+\sqrt{2})^k : k \in \mathbb{Z}\}$.

Ring of Integers and Unit Group

The ring of integers $\mathcal{O}_K$ of a number field K is the ring of all algebraic integers contained in K.

Example

The ring of integers of $\mathbb{Q}(\sqrt{2})$ is equal to $\mathbb{Z}[\sqrt{2}]$.

The unit group $\mathcal{O}_K^\times$ of the ring of integers is the multiplicative group of elements of $\mathcal{O}_K$ whose inverses lie in $\mathcal{O}_K$.

Example

The unit group of $\mathbb{Z}[\sqrt{2}]$ is $\pm(1+\sqrt{2})^{\mathbb{Z}} = \{\pm(1+\sqrt{2})^k : k \in \mathbb{Z}\}$. Units can be quite unpredictable. For example, the unit group of $\mathbb{Z}[\sqrt{241}]$ is $\pm(71011068 + 4574225\sqrt{241})^{\mathbb{Z}}$.

Units in Pell's Equations

Consider an element $\alpha \in \mathbb{Q}(\sqrt{d})$, $\alpha \notin \mathbb{Q}$.

Units in Pell's Equations

Consider an element $\alpha \in \mathbb{Q}(\sqrt{d})$, $\alpha \notin \mathbb{Q}$.

- The minimal polynomial of α^{-1} is the reciprocal of the minimal polynomial of α.
- Thus, if α is a unit, we must have that the constant coefficient of its minimal polynomial is ± 1.
- If $\alpha = a + b\sqrt{d}$, then its minimal polynomial is $(x - a - b\sqrt{d})(x - a + b\sqrt{d})$ with constant coefficient $a^2 - b^2 d$.

Units in Pell's Equations

Consider an element $\alpha \in \mathbb{Q}(\sqrt{d})$, $\alpha \notin \mathbb{Q}$.

- The minimal polynomial of α^{-1} is the reciprocal of the minimal polynomial of α.
- Thus, if α is a unit, we must have that the constant coefficient of its minimal polynomial is ± 1.
- If $\alpha = a + b\sqrt{d}$, then its minimal polynomial is $(x - a - b\sqrt{d})(x - a + b\sqrt{d})$ with constant coefficient $a^2 - b^2 d$.

Thus, the unit group of $\mathbb{Q}(\sqrt{d})$ helps us completely characterize the solutions to Pell's equations $a^2 - b^2 d = \pm 1$!

Dirichlet's Unit Theorem

For $K = \mathbb{Q}(\alpha)$, let the minimal polynomial of α have r_1 real roots and $2r_2$ complex roots. Here, we denote by (r_1, r_2) the signature of K.

Dirichlet's Unit Theorem

For $K = \mathbb{Q}(\alpha)$, let the minimal polynomial of α have r_1 real roots and $2r_2$ complex roots. Here, we denote by (r_1, r_2) the signature of K.

Theorem (Dirichlet, 1846)

The unit group $\mathcal{O}_K^\times$ is generated by a cyclic group of roots of unity and $r_1 + r_2 - 1$ independent generators.

Dirichlet's Unit Theorem

For $K = \mathbb{Q}(\alpha)$, let the minimal polynomial of α have r_1 real roots and $2r_2$ complex roots. Here, we denote by (r_1, r_2) the signature of K.

Theorem (Dirichlet, 1846)

The unit group $\mathcal{O}_K^\times$ is generated by a cyclic group of roots of unity and $r_1 + r_2 - 1$ independent generators.

Example

The polynomial $x^3 - 2$ has one real root and two complex roots so the unit group of $\mathbb{Z}(\sqrt[3]{2})$ has rank 1.

Finite Fields

A finite field is a field of finite order.

Finite Fields

A finite field is a field of finite order.

- All finite fields have size p^n for prime p and integer n.
- The multiplicative group of a finite field $\mathbb{F}_q^\times$ is cyclic.

Finite Fields

A finite field is a field of finite order.

- All finite fields have size p^n for prime p and integer n.
- The multiplicative group of a finite field $\mathbb{F}_q^\times$ is cyclic.

Example

As from before, $\mathbb{F}_7$ is a finite field.

Inert Primes and the Reduction Map

A prime p is inert in K if the ideal $p\mathcal{O}_K$ is prime.

Inert Primes and the Reduction Map

A prime p is inert in K if the ideal $p\mathcal{O}_K$ is prime.

- There is a natural reduction map $\phi_p : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$ given by reducing elements of $\mathcal{O}_K$ modulo $p\mathcal{O}_K$.
- In the case where p is inert, we see that $\mathcal{O}_K/p\mathcal{O}_K$ is a field.
- We have that $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_{p^n}$, where n is the degree of K.

Possible Images of the Unit Group

We consider the following problem:

Possible Images of the Unit Group

We consider the following problem:

Question

For a rational prime p, positive integer n, what subgroups of $\mathbb{F}_{p^n}^{\times}$ are realizable as the image of the unit group of a number field under reduction modulo p?

Possible Images of the Unit Group

We consider the following problem:

Question

For a rational prime p, positive integer n, what subgroups of $\mathbb{F}_{p^n}^\times$ are realizable as the image of the unit group of a number field under reduction modulo p?

Specifically, we consider the map

$$\mathcal{O}_K^\times \to (\mathcal{O}_K/p\mathcal{O}_K)^\times \simeq \mathbb{F}_{p^n}^\times.$$

Example

The subgroup $\{\pm 1\}$ of $\mathbb{F}_{25}^\times$ can be realized as the image of the unit group of $\mathbb{Q}(\sqrt{231})$, since the unit group is $\pm(76 + 5\sqrt{231})^{\mathbb{Z}}$. Under reduction modulo 5, this becomes $\pm 1^{\mathbb{Z}}$.

Results on the Maximal Image and Quadratic Case

For odd prime p, define the subgroup $U_{\mathbb{F}_{p^n}^\times}$ to be the subgroup of index $(p-1)/2$ in the cyclic group $\mathbb{F}_{p^n}^\times$.

Results on the Maximal Image and Quadratic Case

For odd prime p, define the subgroup $U_{\mathbb{F}_{p^n}^\times}$ to be the subgroup of index $(p-1)/2$ in the cyclic group $\mathbb{F}_{p^n}^\times$.

Theorem

The largest subgroup of $\mathbb{F}_{p^n}$ attainable as an image of the reduction map on the group of units of a number field in which p is inert is $U_{\mathbb{F}_{p^n}^\times}$, occuring for infinitely many number fields K.

Results on the Maximal Image and Quadratic Case

For odd prime p, define the subgroup $U_{\mathbb{F}_{p^n}^\times}$ to be the subgroup of index $(p-1)/2$ in the cyclic group $\mathbb{F}_{p^n}^\times$.

Theorem

The largest subgroup of $\mathbb{F}_{p^n}$ attainable as an image of the reduction map on the group of units of a number field in which p is inert is $U_{\mathbb{F}_{p^n}^\times}$, occuring for infinitely many number fields K.

In the case where $n = 2$, the signature is either $(0, 1)$ (complex quadratic number field) or $(2, 0)$ (real quadratic number field). In the second case, we have the following complete result:

Theorem

Every subgroup of $U_{\mathbb{F}_{p^2}^\times}$ is attainable as the image of the reduction map on the group of units of a real quadratic number field in which p is inert.

Generalization to Fields of Higher Degree

Considering our results in the real quadratic case, we conjecture the following generalization:

Conjecture

Every subgroup of $U_{\mathbb{F}_{p^n}^\times}$ is attainable as the image of the reduction map on the group of units of a number field of degree n and specified signature (r_1, r_2) in which $r_1 + r_2 - 1 > 0$.

Orders

An order $\mathcal{O}$ of a number field K is a subring of K that is finitely generated (as a $\mathbb{Z}$-module) for which the field of fractions of $\mathcal{O}$, or $\{\alpha/\beta : \alpha, \beta \in \mathcal{O}\}$, is equal to K.

Orders

An order $\mathcal{O}$ of a number field K is a subring of K that is finitely generated (as a $\mathbb{Z}$-module) for which the field of fractions of $\mathcal{O}$, or $\{\alpha/\beta : \alpha, \beta \in \mathcal{O}\}$, is equal to K.

Example

As from before, $\mathcal{O}_K$ is an example of an order of K. We also have that $\mathbb{Z}[\sqrt{8}]$ is an order of $\mathbb{Q}(\sqrt{2})$. By containment, it is "smaller" than $\mathbb{Z}[\sqrt{2}]$.

Orders generalize the notion of the ring of integers.

Orders

An order $\mathcal{O}$ of a number field K is a subring of K that is finitely generated (as a $\mathbb{Z}$-module) for which the field of fractions of $\mathcal{O}$, or $\{\alpha/\beta : \alpha, \beta \in \mathcal{O}\}$, is equal to K.

Example

As from before, $\mathcal{O}_K$ is an example of an order of K. We also have that $\mathbb{Z}[\sqrt{8}]$ is an order of $\mathbb{Q}(\sqrt{2})$. By containment, it is "smaller" than $\mathbb{Z}[\sqrt{2}]$.

Orders generalize the notion of the ring of integers.

- The ring of integers is the maximal order of K.
- Dirichlet's unit theorem holds for orders as well, so the structure of the unit group of an order $\mathcal{O}^\times$ is well known.

Results for an Order

With the notion of orders, we may change the conditions of our problem, instead fixing a number field K and odd prime p inert in K, then varying our choice of order $\mathcal{O}$ and looking at its unit group.

Results for an Order

With the notion of orders, we may change the conditions of our problem, instead fixing a number field K and odd prime p inert in K, then varying our choice of order $\mathcal{O}$ and looking at its unit group.

We will say that for a number field K of degree n a prime p remains inert in an order $\mathcal{O}$ if $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^n}$.

Results for an Order

With the notion of orders, we may change the conditions of our problem, instead fixing a number field K and odd prime p inert in K, then varying our choice of order $\mathcal{O}$ and looking at its unit group.

We will say that for a number field K of degree n a prime p remains inert in an order $\mathcal{O}$ if $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^n}$.

Theorem

For a real quadratic number field K and prime p inert in K, let the image of the unit group of $\mathcal{O}_K^\times$ under reduction modulo p be a subgroup U of $U_{\mathbb{F}_{p^2}^\times}$. Then, for every subgroup $S \leq U$, there exists an order $\mathcal{O}$ of K in which p remains inert and the reduction of $\mathcal{O}^\times$ modulo p is the subgroup S.

Generalization to Fields of Higher Degree

Considering our results in the real quadratic case, we conjecture the following generalization for orders:

Considering our results in the real quadratic case, we conjecture the following generalization for orders:

Conjecture

For a number field K of degree n and prime p inert in K, let the image of the unit group of $\mathcal{O}_K^\times$ under reduction modulo p be a subgroup U of $U_{\mathbb{F}_{p^n}^\times}$. Then, for every subgroup $S \leq U$, there exists an order $\mathcal{O}$ of K in which p remains inert and the reduction of $\mathcal{O}^\times$ modulo p is the subgroup S.

Acknowledgements

- I would like to give special thanks to my mentor Dr. Alexander Petrov for proposing this topic, and for the guidance and resources he provided me throughout the research period.
- I would also like to thank the PRIMES-USA program and its organizers for providing me with this research opportunity.