Algebraic Number Theory and Representation Theory

MIT PRIMES Reading Group

Jeremy Chen and Tom Zhang (mentor Robin Elliott)

December 2017

Algebraic Number Theory

Definition

An algebraic number is a complex number that is a root of a polynomial over the rationals.

- If it satisfies a monic polynomial over the integers, it is called an algebraic integer.
- The algebraic numbers form a field, while the algebraic integers form a ring.

Algebraic Number Fields

- Given an algebraic number α, we can create a new set $\mathbb{Q}[\alpha]$ of all polynomials over $\mathbb{Q}$ evaluated at α.
- This creates a field, called an algebraic number field.

Quadratic Fields

Definition

Quadratic fields are fields of the form $\mathbb{Q}[\sqrt{d}]$, where d is a nonzero, squarefree integer.

- It can be either a real or imaginary field– we tended to focus on imaginary fields, as they are much easier to work with.
- The integers in this field are either of the form $a + b\sqrt{d}$, where a and b are integers and d is 2 or 3 mod 4, or $a + b(\frac{1+\sqrt{d}}{2})$ if d is 1 mod 4.

Unique Prime Factorization over Imaginary Quadratic Fields

- Much like in the integers, we can define primes in quadratic fields.
- We can also define unique prime factorization– every number factorizes uniquely into primes up to units.
- For imaginary quadratic fields, other than 1 and -1, the units are i and -i for d=-1, and $\frac{\pm 1 \pm \sqrt{-3}}{2}$ for d=-3. For real quadratic fields, there are an infinite amount of units.
- Unique prime factorization in imaginary fields only occurs for d=-1, -2, -3, -7, -11, -19, -43, -67, and -163. For real quadratic fields, this is still an open question.

Fermat's Last Theorem for $n = 3$

- We proved Fermat's Last Theorem for a special case, $n = 3$.
- We did this by proving that it could not hold over $\mathbb{Q}[\sqrt{-3}]$, and even showing a stronger statement that there do not exist integers in the field a, b, and c, a unit e, and a rational integer r, such that $a^3 + b^3 + e((\sqrt{-3})^r c)^3 = 0$.
- The way we did this was proof by descent– we showed that if there was was a solution (a, b, c), and it was the solution such that $N(a^3 b^3 (\sqrt{-3})^{3r} c^3)$ was smallest, then a solution (x_1, x_2, x_3) with $N(x_1^3 x_2^3 (\sqrt{-3})^{3r-3} x_3^3) < N(a^3 b^3 (\sqrt{-3})^{3r} c^3)$ exists, a contradiction.

Ideals

Definition

Given a ring R, an ideal I is a subset of R such that I is closed under addition, and for all r in R and i in I, ir is in I.

Example

The even integers in the ring of integers form an ideal.

- Ideals factor uniquely into prime ideals all quadratic fields. This allows us to construct similar properties to those of the integers.
- A prime ideal is an ideal I such if a and b are in R and ab is in I, then either a was in I or b was in I.
- A fractional ideal is a ideal with all elements divided by a specific algebraic integer.

Example

The multiples of $\frac{1}{2}$ form a fractional ideal.

The Ideal Class Group

- Two ideals A and B in a ring are equivalent if there exist algebraic integers a, b such that $aA = bB$.
- This equivalence relation creates a finite set of equivalence classes, called the ideal class group.

Example

In $\mathbb{Q}[\sqrt{-5}]$, the class group is the class of principal ideals and ideals congruent to $(2, 1+\sqrt{-5})$.

- If the ideal class group has order 1, then the field it is over has unique prime factorization.
- We can find the classes of the ideal class group through the Minkowski bound.

Equations of the form $x^2 + k = y^3$

- Using prime factorization of ideals in quadratic fields and the ideal class group, we can solve these types of equations for some positive integers k.
- An example is $k = 5$; we first use normal number theory to show y is odd and x is even, and that x and y are coprime.
- Factoring into ideals gets $(x + \sqrt{-5})(x - \sqrt{-5}) = (y)^3$, and they are also coprime ideals.
- In ideals, we then must have that both ideals are cubes of other ideals, so $(x + \sqrt{-5}) = a^3$, where a is an ideal.
- Since $\mathbb{Q}[\sqrt{-5}]$ has class number 2, a is principal, so we have $x + \sqrt{-5} = (b + c\sqrt{-5})^3$, for some rational integers b and c.
- This gets the equation $c(3b^2 - 5c^2) = 1$, which has no solutions.

Representation Theory

- Groups: Symmetries
- Matrices: Linear Transformations (also symmetries)
- Representation Theory: the relationship between these two

Definition of Representations

Definition

A Representation is a homomorphism $\rho : G \to GL(V)$ where G is a group, $GL(V)$ is the group of invertible linear operators over a vector space V.

- Homomorphism means: $\forall a, b \in G, \rho(a)\rho(b) = \rho(ab)$

Irreducible Representations

- In some sense: $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} = A + B$

Definition

A representation $\rho : G \to GL(V)$ is irreducible if there's no proper subspace W of V such that W is fixed by G: that is, $\forall g \in G, \rho(g)(W) \subset W$.

- All representations break into them.

Characters

- All matrices corresponding to one conjugacy class have the same trace (Left as an exercise)
- We call those traces the character of a representation.
- The character of a representation uniquely identifies the representation.
- There are as many irreducible characters as conjugacy classes. Which turns our search for irreducible representations into filling out the character table.

Inner Product of Characters

Definition

The inner product of two characters is defined by

$$< \chi, \chi' >= \frac{1}{|G|} \sum_{g \in G} \chi(g) \chi'(g^{-1})$$

- For irreducible ρ and ρ', $< \rho, \rho' >= 0$ iff $\rho \neq \rho'$
- Irreducibility Criterion: $< \rho, \rho >= 1$ iff ρ is irreducible

Example: S_4

The group of all permutations on four elements

First find conjugacy classes

	Size	1	6	3	6	8
Representations		()	(ab)	(ab)(cd)	(abcd)	(abc)

Trivial Permutation

	Size	1	6	3	6	8
Representations		()	(ab)	(ab)(cd)	(abcd)	(abc)
Trivial	ρ_1	1	1	1	1	1

Sign Representation

	Size	1	6	3	6	8
Representations		()	(ab)	(ab)(cd)	(abcd)	(abc)
Trivial	ρ_1	1	1	1	1	1
Sign	ρ_2	1	-1	1	-1	1

What next?

	Size	1	6	3	6	8
Representations		()	(ab)	(ab)(cd)	(abcd)	(abc)
Trivial	ρ_1	1	1	1	1	1
Sign	ρ_2	1	-1	1	-1	1

Permutation Representation

	Size	1	6	3	6	8
Representations		()	(ab)	(ab)(cd)	(abcd)	(abc)
Trivial	ρ_1	1	1	1	1	1
Sign	ρ_2	1	-1	1	-1	1
Permutations	ρ_3	3	1	-1	-1	0

Permutation Representation

	Size	1	6	3	6	8
Representations		()	(ab)	(ab)(cd)	(abcd)	(abc)
Trivial	ρ_1	1	1	1	1	1
Sign	ρ_2	1	-1	1	-1	1
Permutations	ρ_3	3	1	-1	-1	0
$\rho_2 \otimes \rho_3$	ρ_4	3	-1	-1	1	0
?						

Permutation Representation

	Size	1	6	3	6	8
Representations		()	(ab)	(ab)(cd)	(abcd)	(abc)
Trivial	ρ_1	1	1	1	1	1
Sign	ρ_2	1	-1	1	-1	1
Permutations	ρ_3	3	1	-1	-1	0
$\rho_2 \otimes \rho_3$	ρ_4	3	-1	-1	1	0
Solve Equations	ρ_5	2	0	2	0	-1