MAT482 Lecture Notes

Arky!! :3c

'24 Fall Semester

Contents

§1 Day 1: Introduction to Class (Sep. 3, 2024)

Class administration notes;

- Prof. Ila (she prefers to be called Ila) will be in Montreal once in a while.
- Masks should be worn if attending lectures in person.
- All reference material for the class can be found on here, or in the UofT library.
- This class will be held in a more experimental teaching style; specifically with the Tuesday discussions.
- Prof. Ila prefers to be contacted on Zulip instead of mail.

To start, this class is on arithmetic statistics, whcih studies "arithmetic objects." Examples of such objects interesting from a number theory perspective include

- Fields, specifically finite extensions of $\mathbb{Q}$ (number fields),
- Binary quadratic forms, i.e. $f(x, y) = ax^2 + bxy + cy^2$,
- Varieties over $\mathbb{Z}$, i.e. zero sets of polynomials with integer coefficients,
- Ideal class groups,
- Primes.

Composition laws can be described as equipping a set with group operations; for example, let us consider the $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms; given $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have $\gamma f(x, y) = f((x, y)\gamma)$.

Exercise 1.1. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, prove that $\mathrm{disc}(f(x, y)) = \mathrm{disc}(\gamma \cdot f(x, y))$. Specifically, the discriminant of $\mathrm{disc}(ax^2 + bxy + cy^2) = b^2 - 4ac$.

Exercise 1.2. Any polynomial Δ in a, b, c satisfying $\Delta(f(x, y)) = \Delta(\gamma \cdot f(x, y))$ is a multiple of the discriminant, or is constant.

§2 Day 2: Course Overview (Sep. 4, 2024)

To start, recall that a binary quadratic form is given by $f(x, y) = ax^2 + bxy + cy^2$, where a, b, c are in some number field, preferably working in $\mathbb{Z}$. We say that $f(x, y) \sim g(x, y)$ if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $g(x, y) = f((x, y)\gamma^T)$ (notational convention).

§2.1 Week 2

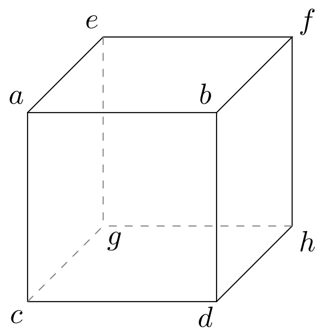
Theorem 2.1 (Gauss)**.** Equivalence classes of binary quadratic forms of a fixed discriminant D form a finite abelian group.

Specifically, $\mathrm{disc}(f(x, y)) = b^2 - 4ac$. The narrow class group is a variant of the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$, of which the latter should be interpreted as the class group of quadratic field $\mathbb{Q}(\sqrt{D})$. This is equal to the fractional ideals of $\mathbb{Q}(\sqrt{D})$ modulo the principal ideals of $\mathbb{Q}(\sqrt{D})$. If $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$ is trivial, then there is unique factorization; otherwise, it has unique factorization of ideals into prime ideals.

Theorem 2.2. This aforementioned finite abelian group is isomorphic to the narrow class group of $\mathbb{Q}(\sqrt{D})$, where D is the discriminant.

§2.2 Week 3

This week will introduce the Bhargava cube, where



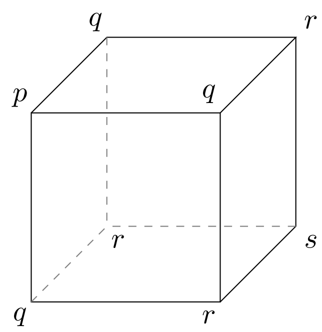
Taking pairs of opposite faces, we obtain 3 pairs of 2×2 matrices that we may use to obtain 3 binary quadratic forms, such as

$$Q_1(x, y) := \det \begin{pmatrix} ax - ey & bx - fy \\ cx - gy & dx - hy \end{pmatrix},$$

with similar definitions for $Q_2(x, y)$ and $Q_3(x, y)$; we may note that Q_1, Q_2, Q_3 have the same discriminant. These induce a cube law where $[Q_1] \cdot [Q_2] \cdot [Q_3]$ is the identity equivalence class. This reinterprets Gauss' composition law. In particular, we may construct a bijection between the equivalence classes of cubes with discrminant D, and the ideal classes (I_1, I_2, I_3) with $I_1 \cdot I_2 \cdot I_3 \subseteq S_p$.

§2.3 Week 4

We construct a symmetric Bhargava cube, where all six of the matrices obtained are symmetric; such a construction follows,



This yields a binary cubic form $px^3 + 3qx^2y + 3rxy^2 + sy^3$, and it induces a bijection from the $\mathrm{SL}_2(\mathbb{Z})$ equivaelnce class of binary cubic forms of discriminant D to the 3-torsion ideal class elements of quadratic rings $S_p = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$. The discriminant formula may be obtained with Viete's formulas and by taking the product over the difference of roots pairwise.

§2.4 Week 5 - Higher Composition Laws

Theorem 2.3 (Levi, Delone-Fadeev, Gan-Gross-Savin)**.** Let us have binary cubic forms $f(x, y) = ax^3+bx^2y+cxy^2+dy^3$ over $\mathbb{Z}$; then $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ acts on f by $\gamma f(x, y) = \frac{f((x,y)\gamma)}{\det \gamma}$. This induces a bijection between $\mathrm{GL}_2(\mathbb{Z})$ orbits of binary cubic forms of a given discriminant D with cubic rings (rank 3 as a $\mathbb{Z}$-module) up to ring isomorphism.

Theorem 2.4 (Davenport-Heilbronn)**.** There is something that bijects to maximal cubic rings at p. (will be expanded in class later on)

A cubic ring is maximal if and only if it is maximal at all primes p; it is maximal at p if and onyl if $R \otimes \mathbb{Z}_p$ is maximal.

§2.5 Week 6

This week we will introduce 3 new parameterizations and composition laws.

1. $2 \times 3 \times 3$ boxes, which induce a bijection between pairs of 3×3 matrices and pairs of ideal class elements I_1, I_2 such that $I_1, I_2 \subseteq R$; i.e., $N(I_1) \cdot N(I_2) = 1$.

2. Symmetrized $2 \times 3 \times 3$ boxes, which induce a bijection between pairs of 3×3 symmetric matrices and order 2 ideal class elements.

3. Bijection between binary n-ic forms and certain rings of rank n.

Specifically, quadratic rings are parametrized by the discriminant, cubic rings by binary cubic forms, and quartic rings by pairs of 3×3 symmetric matrices, with extra structure in resolvent rings.
If Q is a quartic ring, it is a rank 4 $\mathbb{Z}$-module,

$$Q = \langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$$

with basis as a $\mathbb{Z}$-module.

Theorem 2.5. To every quartic ring Q, there is a resolvent cubic ring $R = \langle 1, \beta_1, \beta_2 \rangle$ and a map $Q/\mathbb{Z} = \langle \alpha_1, \alpha_2, \alpha_3 \rangle \to R/\mathbb{Z} = \langle \beta_1, \beta_2 \rangle$.

§2.6 Week 7

Theorem 2.6 (Bhargava)**.** There is a bijection between $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ equivalence classes of ternary quadratic forms and (Q, R) (quartic rings and cubic resolvents).

§2.7 Week 8 and Onwards

We will look at which quartic rings are parametrized by binary quartic forms (Wood), and introduce the Davenport-Heilbronn theorem properly (?); the number of cubic fields ordered by discriminant is given by

$$\frac{1}{3\zeta(3)}x + o(x).$$

Then we will talk about Prof. Ila's research.