Number Theory/Representation Theory Notes
Robbie Snellman
ERD Spring 2011

January 27
Speaker: Moshe Adrian

Number Theorist Perspective: Number theorists are interested in studying $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. One way to study any group is to study the group's representations.

Definition. *A representation of a group G is a homomorphism $G \longrightarrow \mathrm{GL}(V)$ where V is a $\mathbb{C}$-vector space. Recall that $\mathrm{GL}(V)$ is the General Linear Group.*

Representation Theorist Perspective: Representation theorists are interested in studying representations of an arbitrary group.

Example. *Some basic groups which are of interest are $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$, $\mathrm{U}(n)$, ...*

It turns out that number and representation theoretic ideas are intimately related. Understanding this relationship is the primary goal of the Langland's Program.

Quick Review: $\mathbb{R}$ and $\mathbb{Q}_p$ are examples of local fields, in particular $\mathbb{R}$ and $\mathbb{Q}_p$ are completions of $\mathbb{Q}$ with respect to different absolute values, namely $|\cdot|_{\mathbb{R}}$ which is an Archimedean absolute value, and $|\cdot|_{\mathbb{Q}_p}$ which is a non-Archimedean absolute value.

Definition. *The p-adic absolute value is defined as follows: let p be a prime and let $x \in \mathbb{Q}$ be written as $x = p^r \frac{m}{n}$, where $(m,p) = (n,p) = 1$. Then,*

$$\left| p^r \frac{m}{n} \right|_p = \frac{1}{p^r}.$$

Hasse-Principle: To understand most problems along $\mathbb{Q}$ it is sometimes enough to understand the analogous problem over $\mathbb{R}$ and $\mathbb{Q}_p$, for every prime p. Therefore, to study representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ we can try to study representations of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ and $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$. Once the solutions in $\mathbb{Q}_p$ and $\mathbb{R}$ are known we essentially patch those solutions together to learn something about $\mathbb{Q}$.

Representation Theory Question. *Given a matrix group G (like $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{Q}_p), \ldots$) is how can we parameterize representations of G?*

Notation. *To specify the notation of a group over a particular field we use $G(\mathbb{R})$, $G(\mathbb{C})$, $G(\mathbb{Q}_p)$.*

1 First Attempt

The first attempt to answer the above question was to let F be either $\mathbb{R}$ or $\mathbb{Q}_p$ and consider the following:

$$\{\text{Representations of } G(F)\} \longleftrightarrow \left\{\text{Representations of } \mathrm{Gal}(\overline{F}/F)\right\}$$

Unfortunately, this attempt has many problems, namely

1. There is no G on the right hand side.
2. If $F = \mathbb{R}$, the right hand side is trivial. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2$.

$$\{\mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathrm{GL}(V)\} \longleftrightarrow ?$$
$$\{\mathrm{SL}_n(\mathbb{R}) \longrightarrow \mathrm{GL}(V)\} \longleftrightarrow ?$$
$$\{\mathrm{SL}_n(\mathbb{Q}_p) \longrightarrow \mathrm{GL}(V)\} \longleftrightarrow ?$$

Solution. *It was quickly realized that a new approach was needed which led to the definition of something called the Weil Group of a field F, denoted W'_F. This object is highly complicated to define, therefore, we omit the details at this point and provide some examples.*

Example. *1. If $F = \mathbb{R}$: $W'_{\mathbb{R}} = \langle \mathbb{C}^\times, j \rangle$ such that $jzj^{-1} = \overline{z}$ for all $z \in \mathbb{Z}^\times$ and $j^2 = -1$. This Weil group is related to the Galois group by the exact sequence*

$$1 \longrightarrow \mathbb{C}^\times \longrightarrow W'_{\mathbb{R}} \longrightarrow \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \longrightarrow 1$$

2. If $F = \mathbb{Q}_p$, then $W'_{\mathbb{Q}_p}$ is more complicated.

2 Second Attempt

The second attempt in trying to answer the above Representation Theory Question was to try and find a correspondence

$$\{\text{Representations of Galois Groups}\} \longleftrightarrow \{\text{Representations of Matrix Groups}\}$$

This attempt brought about what is known as the Local Langland's Correspondence for $\mathrm{GL}_n(F)$ which is

$$\{G(F) \longrightarrow \mathrm{GL}(V)\} \longleftrightarrow \{W_F' \longrightarrow \mathrm{GL}(W)\}$$

where W is a vector space over some field. Unfortunately, this attempt cannot be true since there is no G on the right hand side of the correspondence. However, we obtain an immediate result, namely

1. The above correspondence is true if $G = \mathrm{GL}_n(F)$, and satisfies some natural technical conditions. Therefore, we should try to generalize this to arbitrary matrix groups.

Idea: We want to bring G to the right hand side of the above correspondence. To establish this we need to define the Langland's Dual Group.

Definition. *To each group G there is an associated group, called the Langland's Dual Group, denoted L_{G°, which is given by combinatorial data.*

Example. *The G's in the table represent groups and the L_{G° is the associated Langland's Dual Group*

G	L_{G°
$\mathrm{GL}_n(F)$	$\mathrm{GL}_n(\mathbb{C})$
$\mathrm{SL}_n(F)$	$\mathrm{PGL}_n(\mathbb{C})$
$\mathrm{PGL}_n(F)$	$\mathrm{SL}_n(\mathbb{C})$
$\mathrm{Sp}(2n, F)$	$\mathrm{SO}(2n+1, \mathbb{C})$

3 Third Attempt

The third attempt is known as parameterization. Part of $W'_{\mathbb{Q}_p}$ sits inside $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. We are thus led to the following conjecture

Local Langland's Conjecture. *There exists the following correspondence*

$$\{\textit{Finite unions of representations } G(F) \to \mathrm{GL}(V)\} \leftrightarrow \left\{\textit{Homomorphisms } W_F' \to L_{G^\circ} \rtimes \mathrm{Gal}(\overline{F}/F)\right\}$$

where the set on the right must satisfy some technical conditions. In many cases the semi-direct product is actually a direct product.

Terminology: The finite union of representations is often called L-packets in the literature.
Concluding Remarks:

1. This particular area of interest seems to be related to most pure branches of mathematics.

2. The Local Langland's Conjecture has been proven in some special cases (completely for $F = \mathbb{R}$) which is due to Langland's himself. Another case where the conjecture has been proven is for the $\mathrm{GL}_n(F)$ case (due to Harris, Taylor, and Hennrart).

February 3
Speaker: Gordan Savin

Let $\zeta_p = e^{2\pi i/p}$ be a primitive p-th root of unity, namely $\zeta^p = 1$ and $\zeta^k \neq 1$ for any $1 \leq k < p$. We will be interested in studying the field $\mathbb{Q}(\zeta_p)$, which is called a cyclotomic field extension. Consider the following:

$$0 = x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + x + 1).$$

We call $x^{p-1} + x^{p-2} + \ldots + x + 1$ the p-th cyclotomic polynomial and denote it $\Phi_p(x)$. By Galois theory we know that $\mathbb{Q}(\zeta_p)$ is Galois since it is the splitting field for $\Phi_p(x)$.

Question. *What is* $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$*?*

Solution. *Notice that any automorphism* $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ *is determined by what it does to* ζ_p*. We consider the following mapping*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/p)^\times$$

by defining $\sigma(\zeta_p) = \zeta_p^k$ *for some* $k \in (\mathbb{Z}/p)^\times$*. We observe that this mapping is a homomorphism since*

$$(\zeta_p^k)^l = \zeta_p^{kl}$$

where kl *is computed in* $\mathbb{Z}/p$*. Moreover, the trivial automorphism* σ_{id} *fixes* ζ_p*, thus* $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/p)^\times$*. Moreover,* $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] == p-1$*, which is the degree of* $\Phi_p(x)$*, and since* $|\,(\mathbb{Z}/p)^\times\,| = p-1$ *we necessarily have that the above mapping is an isomorphism. Therefore, the Galois group of* $\mathbb{Q}(\zeta_p) \supset \mathbb{Q}$ *is* $(\mathbb{Z}/p)^\times$*.*

More work is needed to show that

$$\mathrm{Gal}(\mathbb{Q}_{\zeta_n}/\mathbb{Q}) \simeq (\mathbb{Z}/n)^\times.$$

A deep theorem in Class Field Theory is that the above extensions constitute all abelian extensions. The theorem is due to Kronecker and Weber and is stated as follows:

Theorem 1. *(Kronecker-Weber) Every finite abelian extension of* $\mathbb{Q}$ *is contained in a cyclotomic extension.*

We now turn our attention to the task of constructing abelian extensions of the complex quadratic field $\mathbb{Q}(i) \subset \mathbb{C}$.

4 Elliptic Curves

We approach this problem by studying elliptic curves as Riemann Surfaces. Let L be a lattice, then an elliptic curve E is defined as $E = \mathbb{C}/L$. Topologically, elliptic curves are products of circles.

Each quadratic complex field gives a lattice ($\mathbb{Q}(i)$ has the lattice $\mathbb{Z}[i]$).

Definition. *We define the Weierstrauss $\wp$-function as* $\wp(z) = \frac{1}{z^2} + \sum_{w \in L \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$

If we take $z \in \mathbb{C}/L$ and consider $z \mapsto (\wp(z), \wp'(z)) \in \mathbb{C}^2$ we see that these are precisely the points satisfying the cubic equation $y^2 = 4x^3 + px + q$.

Example. *We can use the cubic equation $y^2 = x^3 + x$ to construct abelian extensions of $\mathbb{Q}(i)$.*

If we attach p-torsion points, for p a prime, to the curve $y^2 = x^3 + x$ we will obtain an abelian extension of $\mathbb{Q}(i)$.

Given an elliptic curve E we consider the endomorphisms of E, denoted $\mathrm{End}(E)$. Clearly $\mathbb{Z} \subset \mathrm{End}(E)$ by considering $x \in E$, $x \mapsto nx$ for $n \in \mathbb{Z}$. For $\mathbb{C}/\mathbb{Z}[i]$, multiplication of i will simply permute the Gaussian lattice, therefore, $\mathrm{End}(E) = \mathbb{Z}[i]$.

Take a pair $(x, y) \mapsto (-x, iy)$, this transformation will preserve the elliptic curve since

$$\begin{aligned} (iy)^2 &= (-x)^3 + (-x) \\ -y^2 &= -x^3 - x \\ y^2 &= x^3 + x. \end{aligned}$$

The automorphism, multiplication by i can be described by the Weierstrauss function defined above.

Let F be an algebraic extension of $\mathbb{Q}(i)$, if $\sigma \in \mathrm{Gal}(F/\mathbb{Q}(i))$, then σ acts on $E(p)$, the p-torsion points of E. This action commutes with the Galois action, namely σ commutes with multiplication by i. In particular $E(p) \simeq \mathbb{F}_p^2$. Moreover, $\mathbb{Z}[i]$ acts on $E(p)$ so $\mathbb{Z}[i]/(p) = \mathbb{F}_p[i]$ acts on $E(p)$.

By definition $\mathbb{F}_p[i] = \mathbb{F}_p \cdot 1 + \mathbb{F}_p \cdot i$, multiplication by $a + bi$ on the basis $\{1, i\}$ gives the matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

Theorem 2. *Let* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be a* 2×2 *matrix that commutes with* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$*, then* $d = a$*,* $c = -b$*.*

The proof of the proposition is an elementary exercise in matrix multiplication and is left to the reader.

The element σ will be given by a matrix commuting with i, hence of the form $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ so

$$\mathrm{Gal}(F/\mathbb{Q}(i)) \subset \mathbb{F}_p[i]^\times = \begin{cases} \mathbb{F}_{p^2}^\times, \text{ if } p \equiv 3 \pmod 4 \\ (\mathbb{F}_p^\times)^2, \text{ if } p \equiv 1 \pmod 4 \end{cases}.$$

February 10
Remi Lodh

5 Algebraic Varieties

Definition. *Let k denote a field (such as $\mathbb{Q}, \mathbb{R}, \mathbb{C} \ldots$). Consider projective n-space denoted*

$$\mathbb{P}^N(k) = \{[a_0 : a_1 : \ldots : a_N] : a_i \in k, \text{ some } a_j \neq 0\}/\sim$$

where $\sim$ is given by $[a_0 : a_1 : \ldots : a_N] \sim [a_0\lambda : a_1\lambda : \ldots : a_N\lambda]$ for all $\lambda \in k^\times$.

Looking at the complex points $k = \mathbb{C}$, one gets a complex manifold $\mathbb{P}^N(\mathbb{C})$.

Let $F_1, F_2, \ldots, F_r$ be homogeneous polynomials is variables $X_0, X_1, \ldots, X_N$, with coefficients in k. Consider the set of points in projective space where all polynomials vanish simultaneously.

Definition. *We define the set of common zeros of the polynomials F_i (called an algebraic variety) to be*

$$V(k) = \{x \in \mathbb{P}^N(\mathbb{C}) : F_i(x) = 0 \text{ for all } i\}$$

In particular, $V(\mathbb{C}) \subset \mathbb{P}^N(\mathbb{C})$. $V(\mathbb{C})$ is a topological space with the subspace topology and may not be a complex manifold.
Goal: Study $V(\mathbb{Q}) \subset V(\mathbb{C})$.

Example. *Let $F_n = X_0^n + X_1^n + X_2^n$ for some $n \in \mathbb{N}$. Define $C_n(\mathbb{C}) = \{x \in P^2(\mathbb{C}) : F_n(x) = 0\}$, called a Fermat Curve. Fermat's Last Theorem states that $C_n(\mathbb{Q}) = \varnothing$ for n-even, $n \geq 4$, or more precisely: $F_n = 0$ has no solution in the rationals if $X_0X_1X_2 \neq 0$, and $n \geq 3$.*

6 Algebraic Curves

Definition. *An algebraic curve is an algebraic variety with one complex dimension (2 real dimensions).*

Example.
1. *Fermat Curve $X_0^n + X_1^n + X_2^n$.*
2. *$E(\mathbb{C}) = \{x \in P^2(\mathbb{C}) : P(x) = 0\}$ where $P(X_0, X_1, X_2) = X_2X_1^2 - X_0^3 - X_0X_2^2$. P is called an elliptice curve.*

We will only consider smooth curves (complex manifolds).

6.1 Topological Classification of Smooth Curves

Every curve is homeomorphic to one of $\{\sum_g\}$ for $g \geq 0$, where $\sum_g$ is the genus-g surface. The only algebraic invariant we have is the genus of the curve.

We have the following trichotomy: let g be the genus of some fixed smooth curve C then

	$C(\mathbb{Q})$
$g = 0$	$C(\mathbb{Q}) = \varnothing$ or $C(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$
$g = 1$	$C(\mathbb{Q}) = \varnothing$ or $C(\mathbb{Q})$ is a finitely generated abelian group
$g > 1$	$C(\mathbb{Q})$ is finite

Case $g = 1$: C is an elliptic curve (assume set of rational points is $\neq \varnothing$). Consider the complex points $C(\mathbb{C}) = \mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, $\mathrm{Im}(\tau) > 0$, e.g. $\tau = i$, then $\mathbb{C}/\mathbb{Z}[i] = E(\mathbb{C})$ in the notation of the previous example.

We know that $C(\mathbb{Q}) = \mathbb{Z}^r \oplus$ finite abelian group. The possibilities for the finite abelian groups was proved by Barry Mazur, the difficult part is determining the rank r of the free part $\mathbb{Z}^r$.

Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q} \subset \mathbb{C}$ and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Studying $C(\mathbb{Q})$ is the same as studying $C(\overline{\mathbb{Q}})$ with the $G_{\mathbb{Q}}$-action, where $G_{\mathbb{Q}}$ is acting on the coordinates of rational points. Unfortunately, we don't know very much about $C(\overline{\mathbb{Q}})$ but we can weaken the problem to studying

$$C(k)[2^n] = \{x \in C(k) : 2^n x = 0\}.$$

Fact: $C(\overline{\mathbb{Q}})[2^n] = C(\mathbb{C})[2^n]$, the 2^n-torsion points in $C(\mathbb{C})$.

Recall that $C(\mathbb{C}) = \mathbb{C}/\Lambda$, so $C(\mathbb{C})[2^n] = \frac{\frac{1}{2^n}\Lambda}{\Lambda} \simeq \Lambda/2^n\Lambda$, so we must have a Galois action on $\Lambda/2^n\Lambda$ since we have a Galois action on $C(\overline{\mathbb{Q}})[2^n]$.

Definition. *Define*

$$T_2(C) = \{(\lambda_n)_{n\in\mathbb{N}} : \lambda_n \in \Lambda/2^n\Lambda,\ 2\lambda_n = \lambda_{n-1}\}$$

$T_2(C)$ is called a Tate Module.

$T_2(C)$ has a $G_{\mathbb{Q}}$ action, we want to study this particular action. As a module $T_2(C) = \mathbb{Z}_2^2$ where

$$\mathbb{Z}_2 = \left\{\sum_{n=0}^{\infty} a_n 2^n : a_n \in \mathbb{Z}\right\}$$

is the 2-adic integers. More generally we could replace 2 by any prime p and consider $T_p(C)$.

Theorem 3. *(Faltings) To know $T_p(C)$ and $G_{\mathbb{Q}}$-action is almost the same as knowing C.*

Stated more precisely

$$\mathrm{Hom}(C_1, C_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathrm{Hom}_{G_{\mathbb{Q}}}(T_p C_1, T_p C_2)$$

So we should be able to recover $r = \mathrm{rank}(C(\mathbb{Q}))$ from $T_p(C)$ and $G_{\mathbb{Q}}$-action.

Local Langland's Conjecture. *(Birch and Swinnerton Dyer) Recipe to recover r from $T_p(C)$ and $G_{\mathbb{Q}}$-action.*

Case $g > 1$: Here $|C(\mathbb{Q})| < \infty$. One can also define $T_p(C)$ and gain more information. There exists a nonabelian version of $T_p(C)$ denoted $\Pi_1^{et}(C)$ or $\Pi_1(C)$ for short, which has a Galois action. For $g = 1$, $\Pi_1(C) = \prod_p T_p(C)$, where $\prod_p$ denotes the product over all primes p.

7 p-adic Integers

Definition. *The p-adic integers are defined as* $\mathbb{Z}_p = \left\{ \sum_{n=0}^{\infty} a_n p^n : a_n \in \mathbb{Z} \} \right\}$.

Definition. *We can define the p-adic rational numbers as* $\mathbb{Q}_p = \mathbb{Z}_p \left[\frac{1}{p} \right]$.

The p-adic numbers are helpful because $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ is far less mysterious than $G_{\mathbb{Q}}$.

Theorem 4. *(Mochizuki) To know $\Pi_1(C)$ with $G_{\mathbb{Q}_p}$-action is the same as knowing $C/\mathbb{Q}_p$.*

Stated more precisely the map

$$\mathrm{Hom}_{dom}(C_1, C_2) \longrightarrow \mathrm{Hom}_{G_{\mathbb{Q}_p}}(\Pi_1(C_1), \Pi_1(C_2))$$

is an isomorphism. The proof of this fact uses something known as p-adic Hodge Theory which we outline as follows:

From a map

$$\Pi_1(C_1) \longrightarrow \Pi_1(C_2)$$

we get a map

$$\left(\mathrm{Hom}^1(\Pi_1(C_1), \mathbb{Q}_p)^*\right)^{G_{\mathbb{Q}_p}} \longrightarrow \left(H^1(\Pi_1(C_2), \mathbb{Q}_p)^*\right)^{G_{\mathbb{Q}_p}}$$

which induces a map

$$\mathbb{P}(H^0(C_1, \Omega'_{C_1})) \longrightarrow \mathbb{P}(H^0(C_2, \Omega'_{C_2}))$$

where C_1 sits inside $\mathbb{P}(H^0(C_1, \Omega'_{C_1}))$ and C_2 sits inside $\mathbb{P}(H^0(C_2, \Omega'_{C_2}))$.