Number Theory

Alexander Paulin

October 25, 2010

Lecture 1

What is Number Theory

Number Theory is one of the oldest and deepest Mathematical disciplines. In the broadest possible sense Number Theory is the study of the arithmetic properties of $\mathbb{Z}$, the integers. $\mathbb{Z}$ is the *canonical* ring. It structure as a group under addition is very simple: it is the infinite cyclic group. The mystery of $\mathbb{Z}$ is its structure as a monoid under multiplication and the way these two structure coalesce. As a monoid we can reduce the study of $\mathbb{Z}$ to that of understanding prime numbers via the following 2000 year old theorem.

Theorem. *Every positive integer can be written as a product of prime numbers. Moreover this product is unique up to ordering.*

This is 2000 year old theorem is the Fundamental Theorem of Arithmetic. In modern language this is the statement that $\mathbb{Z}$ is a unique factorization domain (UFD). Another deep fact, due to Euclid, is that there are infinitely many primes. As a monoid therefore $\mathbb{Z}$ is fairly easy to understand - the free commutative monoid with countably infinitely many generators cross the cyclic group of order 2.

The point is that in isolation addition and multiplication are easy, but together when have vast hidden depth. At this point we are faced with two potential avenues of study: analytic versus algebraic. By analytic I questions like trying to understand the distribution of the primes throughout $\mathbb{Z}$. By algebraic I mean understanding the structure of $\mathbb{Z}$ as a monoid and as an abelian group and how they interact. We shall be taking the algebraic approach.

Reciprocity

Gauss made many fundamental breakthroughs in Number Theory. The one which he is most celebrated for is a well known result called quadratic reciprocity. He himself described it as a golden theorem. I think he proved it when he was 18.

Theorem. *Let p and q be distinct odd primes. The congruence equations*

$$\begin{aligned} x^2 &\equiv p \ \ (mod\ q) \\ x^2 &\equiv q \ \ (mod\ p) \end{aligned}$$

are either both soluble or insoluble except when both p and q are congruent to 3 modulo 4. In this case exactly one is soluble.

This theorem looks innocuous, but it is profound. Observe that under multiplication p and q are completely unrelated. What quadratic reciprocity is saying is that if we throw addition into the mix then they are. Addition and multiplication are interacting in a highly non-trivial way. Another way of viewing quadratic reciprocity is as some independent way of telling whether the congruence $x^2 \equiv p \ \ (mod\ q)$ is soluble. This holds the key to how this result fits into a broader conceptual framework.

Let $f(x)$ be a monic polynomial of degree n with integer coefficients. A very natural question to ask (the Greeks did it) is how to determine the zeros of $f(x)$ in $\bar{\mathbb{Q}} \subset \mathbb{C}$. Up to $f(x)$ of degree 4 this isn't so hard: they are soluble by radicals. For degree 2 we have the quadratic equation. Beyond that things get harder. Galois was the first to truly understand why. Let $E/\mathbb{Q}$ be the minimal subfield of $\bar{\mathbb{Q}}$ containing all the zeros of $f(x)$. This is called the splitting field of $f(x)$ and is formed by *adjoining* its zeros to $\mathbb{Q}$. $E/\mathbb{Q}$ is a finite extension. In fact it is Galois. Any finite field extension is called a number field. Understanding such field extensions is the same as understanding the zeros of $f(x)$, so we've translated the problem into more familiar language. So what we're really interested in is finite field extensions of the rationals. Incidentally all Galois finite field extension of $\mathbb{Q}$ arise in this way.

Don't worry if you don't know what all these words mean. I what to give you an overview. I'll introduce them properly later.

Let $Gal(E/\mathbb{Q})$:= field automorphisms of E fixing $\mathbb{Q}$. This group is finite of oder equal to the dimension of E over $\mathbb{Q}$. The Fundamental Theorem of Algebra tells us that E is formed by adjoing the n (possibly repeated) roots of $f(x)$ to $\mathbb{Q}$. Fix an ordering on these roots. Because any element of $\sigma \in Gal(E/\mathbb{Q})$ fixes $\mathbb{Q}$ we know that it must permute the roots. Hence we get an injective homomorphism $Gal(E/\mathbb{Q}) \to S_n$. Observe that there is no canonical way of doing this so we only obtain a conjuagacy class of subgroups of S_n. Let p be a prime. We may reduce $f(x)$ mod p to give a polynomial with coefficients in $\mathbb{F}_p$. Factor this into it's irreducible in $\mathbb{F}_p[x]$ and let $n_1, ..n_r$ be their degrees. Note that $n_1 + .. + n_r = n$. These numbers naturally give a conjugacy class in S_n, given by permutations with cycle type $(n_1, ...n_r)$. The intersection this conjugacy class with any of the images of $Gal(E/\mathbb{Q})$ in S_n may give more than one conjugacy class in $Gal(E/\mathbb{Q})$. However, if p does not divide the discriminant of $f(x)$ then this conjugacy class is well defined. Hence for all but finitely many primes p we have a well defined conjugacy class which we denote by $frob_p \subset Gal(E/\mathbb{E})$, the frobenius at p. It is a fact that all of this only actually depends on E and p, not on

$f(x)$. The prime p is said to *split completely* in E if is of frobenius class one: that is p does not divide the discriminant and $f(x)$ splits into linear factors in $\mathbb{F}_p[x]$. Let $S(E)$ denote the subset of the primes which split completely in E. We have the following remarkable fact:

Theorem. *The map from number fields to subsets of the primes given by $E \to S(E)$ is injective.*

This is amazing. It tells us that understanding number fields is the same as determining the image of this map. Any independent way of giving a characterization for this image is called a *reciprocity* theorem. Quadratic reciprocity gives us the case when $f(x) = x^2 + p$, so $E = \mathbb{Q}(\sqrt{-p})$. At the end of the nineteen century a categorization was given when $Gal(E/\mathbb{Q})$ is abelian. This was later generalized to what we now call class field theory - a high point of early twentieth century mathematics. In 1967 Robert Langlands proposed a complete reciprocity law. Let me describe the essence of his insight.

Recall that we can spot whether a prime p is contained in $S(E)$ by looking at its frobenius conjugacy class. Conjugacy classes are slippery things so Langlands idea is to consider a faithful representation

$$\rho : Gal(E/\mathbb{Q}) \to GL_m(\mathbb{C}),$$

for some positive integer m. Such a representation is called an Artin representation (after Emile Artin). For any p not dividing the discriminant the image of $frob_p$ gives a semi-simple conjugacy class in $GL_m(\mathbb{C})$. A conjugacy classes in $GL_m(\mathbb{C})$ has a well defined characteristic polynomial. This gives us something solid to play with. For p not dividing the disciminant we define the local L-factor of ρ at p to be the complex analytic function:

$$L_p(\rho, s) = det[I - p^{-s}(\rho(frob_p))]^{-1}.$$

This looks rough but if we choose $f(x) = x$ (so $E = \mathbb{Q}$ then $Gal(E/\mathbb{Q})$ is trivial) and the trivial one dimensional representation then we get

$$L_p(\rho, s) = (1 - p^{-s})^{-1}.$$

Recall that in this case a famous theorem of Euler (and later Riemann) states that the product of all these very simple L-factors gives a meromorphic function on $\mathbb{C}$, and for $Re(s) > 1$ we get

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1},$$

the Riemann zeta function. Taking a cue from this we define the L-function associated to ρ to be the formal product

$$L(\rho, s) = \prod_p{}' L_p(\rho, s).$$

The dash meens we are taking the product only over primes not dividing the discriminant. This in fact can be proven to converge to a meromorphic function on $\mathbb{C}$. An elementary

lemma of Dirichlet tells us that we can recover the local L-factors for each p. Also notice that we can detect from $L_p(\rho, s)$ whether p is contained in $S(E)$. Hence this meromorphic function knows $S(E)$.

We've turned a piece of arithmetic into a piece of analysis. Langlands fundamental insight was there such a function should be naturally associated to another class of object - an automorphic representation. Automorphic representations are totally analytic. Examples of such things are modular forms. This is amazing. He is essentially saying that they provide the key to truly understanding arithmetic. This is the Langlands Philosophy the guiding force behind a vast swath of modern mathematics. Wile's proof of Fermat's Last Theorem involved proving that the L-functions coming from a certain class of Galois representation actually came from modular forms

I wanted to tell you this because the central idea is very elegant and often overlooked in a first course. Clearly there is far too much to cover everything I've said here in any depth. What should be clear is that the language of number fields and Galois groups and their representations is fundamental to this whole picture. It is these that we'll study in the most depth. Hopefully by the end of the course we'll get to automorphic representations.

Number Theory

Alexander Paulin

August 31, 2009

Lecture 2

Number Fields

Throughout this section all rings will be commutative with unit.

Dedekind Domains

A **number field** is a finite field extension $E/\mathbb{Q}$. The simplest example is $\mathbb{Q}$. By construction we have the inclusion $\mathbb{Z} \subset \mathbb{Q}$. $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. It is elementary to show that $\mathbb{Z}$ is a PID, in particular it is Noetherian and all non-zero prime ideals are maximal. This last statement says that it has Krull dimension 1. The Fundamental Theorem of Arithmetic tells us that it is a UFD. A not so obvious property is that $\mathbb{Z}$ is integrally closed. This means that if $\alpha \in \mathbb{Q}$ is a root of a monic polymomial $f \in \mathbb{Z}[X]$ then $\alpha \in \mathbb{Z}$. This is Gauss' Lemma. The key algebraic properties of $\mathbb{Z}$ which we will be interested in are:

1. Noetherian.
2. Integral domain.
3. Integrally closed.
4. Every non-zero prime ideal is maximal.

Obverse that we've left out the fact that $\mathbb{Z}$ is a PID. This motivate the following key definition:

Definition. *A ring R is a Dedekind domain if it satisfies the above four properties.*

Observe that any fields is a Dedekind domain. We want to generalize this to a number field $E/\mathbb{Q}$. First let me remind you about the concept of integral dependence and closure.

Let R be an integral domain (not necessarily Dedekind), K its field of fractions. Let L/K be a finite field extension.

Definition. *The integral closure of R in L is the subset of $S \subset L$ such that $\alpha \in S \iff \exists f \in R[X]$ monic, such that $f(\alpha) = 0$.*

Proposition. *1. S is a subring of L and is hence a domain.*

2. $Frac(S) = L$.

3. S is integrally closed in L.

Proof. The first and second parts are an elementary exercise. A proof of the third can be found in §1, of Chapter 5 of Commutative Algebra volume 1 by Zariski/Samuel. □

Fundamental Fact 1:

Proposition. *Let R be a Dedekind domain, K it's field of fractions. Let L/K be a finite separable extension. Let S be the integral closure of R in L. Then S is a Dedekind domain, $Frac(S) = L$ and S s a finite R-module spanning L over K.*

Proof. This is proposition 1 of §4 of the Local Fields chapter of Cassels/Frohlich. □

The separability is only required for the finiteness property of S as an R-module. We now have the following key definition:

Definition. *Let $E/\mathbb{Q}$ be a finite extension. The ring of integers of E, denoted $\mathcal{O}_E$, is the integral closure of $\mathbb{Z}$ in E.*

Corollary. *Let $E/\mathbb{Q}$ be a number field. The ring of integers $\mathcal{O}_E$ is a Dedekind domain and is finite and free as a $\mathbb{Z}$-module with rank equal to $[E : \mathbb{Q}]$.*

Proof. The first part is immediate by the above proposition and the fact that $\mathbb{Z}$ is a Dedekind domain. $E/\mathbb{Q}$ is automatically separable because $char(\mathbb{Q}) = 0$. Because $\mathcal{O}_E$ is a domain we know that as a $\mathbb{Z}$-module it is finite and torsion free, hence it is free. Because it spans E over $\mathbb{Q}$ we know it must have rank equal to $[E : \mathbb{Q}]$. □

Remarks. *1. If E/F is a finite extension of number fields then the integral closure of $\mathcal{O}_F$ in E is equal to $\mathcal{O}_E$. Hence $\mathcal{O}_E$ is a finitely generated $\mathcal{O}_F$-module. Again it must be torsion free, and by the structure theorem for finitely generated modules over a Dedekind domain it is projective. In general it will not be free.*

2. When we wrote down our initial list of algebraic properties of $\mathbb{Z}$ we did not include that it was a PID. This was because this property is not necessarily preserved under under finite integral closure. For example: Let $E = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_E = \mathbb{Z}[\sqrt{-5}]$. Observe that 6 has two distinct factorisations into irreducibles:

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We see that in this case the ring of integers is not a PID as it is not a UFD. The initial algebraic properties of $\mathbb{Z}$ we listed were singled out precisely because they are preserved by finite integral closure.

Hence we have seen that in general $\mathcal{O}_E$ is not a PID or even a UFD. In fact it is true that for a Dedekind domain being a PID is equivalent to being a UFD. At this point this would seem like a catastrophe - how are we going to come up with the concept of a prime for an arbitrary number field?

Observe though that if R is a PID then there is a natural bijection between prime elements (up to association) and prime ideals: $a \to (a)$. Hence in $\mathbb{Z}$ we could think about prime numbers as prime ideals. Recall a prime ideal is proper by convention. To recover a good concept of primes in a Dedekind domain we will switch from the concept of a prime elements to a prime ideals.

Fractional Ideals

Let R be an integral domain, K it's field of fractions. For R-submodules I_1, I_2 of K we may define the concept of multiplication: $I_1 I_2 \subset K$, generated by products. If I_1 and I_2 are contained in R then they are ideals in the usual sense and this is just multiplication of ideals. In particular, if R is a PID and $I_1 = (a)$ and $I_2 = (b)$, then $I_1 I_2 = (ab)$. We may also define the concept of addition $I_1 + I_2 \subset K$ in the obvious way. If I_1 and I_2 are ideals of R then we say that they are coprime if $I_1 + I_2 = R$.

An R-submodule of K is a *fractional ideal* of R if it is non-zero and there is a non-zero element $a \in R$ such that $aI \subset R$. The simplest example is the free $\mathbb{Z}$-module in $\mathbb{Q}$ generated by a non-zero fraction $a \in \mathbb{Q}$. It is clear that the product of two fractional ideals is again a fractional ideal. The trivial ideal in R is clearly a fractional ideal.

Proposition. *Let R a commutative ring, the following are equivalent:*

1. *R is a Dedekind domain.*
2. *All fraction ideals are invertible. That is, given $I \subset K$, a fractional ideal $\exists J \subset K$ a fractional ideal, such that $IJ = R$.*

Proof. This is proposition 1 of §2 of the Local Fields chapter of Cassels/Frohlich. □

In fact $I^{-1} = \{x \in K | xI \subset R\}$. Hence for R a Dedekind domain, under the operation of multiplication, the fractional ideals of R form an abelian group $\mathfrak{I}(R)$. Observe that if $I \in \mathfrak{I}(R)$ such that $I \subset R$ but $I \neq R$ then I^{-1} is not contained in R.

Fundamental Fact 2:

Theorem. *If R is a Dedekind domain then $\mathfrak{I}(R)$ is free on the non-zero prime ideals of R.*

Proof. This is propostion 2 of §2 of the Local Fields Chapter in Cassels/Frohlich. □

Hence given $I \in \mathfrak{I}(R)$, there is a unique decomposition

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)},$$

where the $v_{\mathfrak{p}}(I) \in \mathbb{Z}$ are zero for all but fintely many $\mathfrak{p}$. Clearly $I \subset R \iff v_{\mathfrak{p}}(I) \geq 0 \ \forall \mathfrak{p}$. Two ideals of R are coprime $\iff$ they share no common prime factor.

Observe that there is a natural homomorphism of abelian groups:

$$\begin{array}{ccc} K^* & \longrightarrow & \mathfrak{I}(R) \\ x & \longrightarrow & (x) \end{array}$$

Here (x) denotes the free R-submodule of K generated by x. The kernel of this map is R^*. The quotient is called the ideal class group of R. We get the exact sequence:

$$1 \to R^* \to K^* \to \mathfrak{I}(R) \to CL(R) \to 1,$$

Where we define $CL(R)$ to be the ideal class group of R. It is an astounding fact, due to L. Claborn, that given any abelian group G, there exists a Dedekind domain such that $CL(R) \cong G$. It is clear from the definition that $CL(R) = 1 \iff R$ is a PID (equivalently a UFD). For number fields we have the following finiteness condition:

Theorem. *For $E/\mathbb{Q}$ a number field, $CL(\mathcal{O}_E)$ is finite.*

Proof. This result is due to Dedekind and Kronecker. It's theorem 50 of The Theory of Algebraic Number Fields by Hilbert. The proof uses Minkowski's approach to the geometry of numbers. □

As we vary across different number fields the behaviour of these groups is very mysterious. We write $h(E) := |CL(\mathcal{O}_E)|$, for the class number of E. Gauss conjectured the following very odd result: the only positive integral values of d such that $h(\mathbb{Q}(\sqrt{-d}) = 1$ are d = 1, 2, 3, 7, 11, 19, 43, 67, 163. This was first proven by a German high school teacher called Kurt Heegner, but no one believe him at first.

It is worth remarking at this point the formal similarity between these ideas and that the Picard group of a smooth projective curve over $\mathbb{C}$. (equivalently a compact Riemann surface). In that setting K is replaced by the field of meromorphic functions on your curve and $\mathfrak{I}(R)$ is the replaced by the divisor group of the curve (the free abelian group on it's closed points). The reason that these two cases are so similar is that the number fields and transcendence degree one extensions of $\mathbb{C}$ share some vary strong algebraic properties. We'll discuss this further then we start talking about completions of a number field.

Number Theory

Alexander Paulin

September 3, 2009

Lecture 3

Relative Extensions

Let E/F be an extension of number field. Let $\mathfrak{P} \subset \mathcal{O}_E$ be a non-zero prime ideal. Recall that it is also maximal.

Proposition. *$\mathfrak{P} \cap \mathcal{O}_F = \mathfrak{p} \subset \mathcal{O}_F$ is a non-zero prime ideal.*

Proof. The fact that $\mathfrak{p}$ is a prime ideal is elementary. To show it is non-zero, let $b \in \mathfrak{P}$ Hence it must be the root of a monic polymomial $f(x) \in \mathcal{O}_F[X]$. Recall that $\mathcal{O}_E$ is a domain hence we may assume that the constant coefficient of $f(x)$ is non-zero. If $f(x) = a_0 + a_1X ... + a_nX^n$ then

$$a_0 = -(a_1b + a_2b^2 + ... + a_nb^n) \in \mathfrak{p}.$$

□

For $E/\mathbb{Q}$ a number field and $\mathfrak{P} \subset \mathcal{O}_E$ a non-zero prime ideal we define the residue field at $\mathfrak{P}$ to be $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_E/\mathfrak{P}$. If E/F is a finite extension of number fields, keeping the above notation, $\mathfrak{P} \cap \mathcal{O}_F = \mathfrak{p}$ then $\mathbb{F}_{\mathfrak{P}}$ is naturally a field extension of $\mathbb{F}_{\mathfrak{p}}$.

Proposition. *$\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is a finite field extension.*

Proof. This follows immediately from the fact that $\mathcal{O}_E$ is a finitely generate $\mathcal{O}_F$-module. □

Proposition. *Let R be a Dedekind domain. Let $I, J \subset R$ be two ideals. Then $I \subset J \iff J|I$.*

Proof. $J|I \Rightarrow I \subset J$ is trivial. Assume that $I \subset J$. Because every fractional ideal of R is invertible we may choose an ideal $J' \subset R$ such that $JJ' = (a)$ for some $a \in R$. Then $IJ' \subset (a)$ so $H = (a^{-1})IJ' \subset R$ is an ideal. Now

$$HJ = (a^{-1})IJ'J = (a^{-1})I(a) = I.$$

□

So in a Dedekind domain inclusion of ideals is the same as division of ideals. Keeping the above notation, if $\mathfrak{p}\mathcal{O}_E \subset \mathcal{O}_E$ is generated by $\mathfrak{p}$ then $\mathfrak{p}\mathcal{O}_E \subset \mathfrak{P}$ and we deduce that $\mathfrak{P}|\mathfrak{p}\mathcal{O}_E$. In this case we say that $\mathfrak{P}$ divides $\mathfrak{p}$, or that $\mathfrak{P}$ lies over $\mathfrak{p}$.

Proposition. *If $\mathfrak{P} \subset \mathcal{O}_E$ is a prime ideal then is divides one and only one prime $\mathfrak{p} \subset \mathcal{O}_F$.*

Proof. By the above we know that $\mathfrak{P}$ divides at least one prime. Assume that $\mathfrak{P}$ divides the distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Note that because these two primes are distinct they are coprime and hence $\mathfrak{p}_1 + \mathfrak{p}_2 = \mathcal{O}_F$. Hence they generate the unit ideal in $\mathcal{O}_E$. By assumption this implies $\mathfrak{P}|\mathcal{O}_E$, a contadiction as $\mathfrak{P}$ is a proper ideal. □

Let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal. Let $\mathfrak{P}|\mathfrak{p}\mathcal{O}_E$. We define the ramification index to be

$$e(\mathfrak{P}/\mathfrak{p}) = v_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_E).$$

Similarly we define the residue class degree to be:

$$f(\mathfrak{P}/\mathfrak{p}) = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}].$$

These behave well with respect to towers of extensions, i.e. if $K/E/F$ are number fields and we have a three primes $\mathcal{P} \in \mathcal{O}_K$, $\mathfrak{P} \subset \mathcal{O}_E$ and $\mathfrak{p} \subset \mathcal{O}_F$ such that $\mathcal{P}|\mathfrak{P}\mathcal{O}_K$ and $\mathfrak{P}|\mathfrak{p}\mathcal{O}_E$, then $e(\mathcal{P}/\mathfrak{p}) = e(\mathcal{P}/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$ and $f(\mathcal{P}/\mathfrak{p}) = f(\mathcal{P}/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$.

We know we may completely factor $\mathfrak{p}\mathcal{O}_E$ as follows:

$$\mathfrak{p}\mathcal{O}_E = \mathfrak{P}_1^{e_1}.....\mathfrak{P}_m^{e_m},$$

for some $m \in \mathbb{N}$, where each $\mathfrak{P}_i$ is a prime ideal of $\mathcal{O}_E$ and $e_i = e(\mathfrak{P}_i/\mathfrak{p})$. For simplicity of notation we write $f_i = f(\mathfrak{P}_i/\mathfrak{p})$.

Theorem. $\sum_{i=1}^{m} e_i f_i = [E : F]$.

Proof. This is proposition 1 of §10 of the Local Fields chapter of Cassels/Frohlich. □

Definition. *Let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal.*

1. *We say that $\mathfrak{p}$ ramifies in $E \iff$ some $e_i > 1$.*
2. *We say the $\mathfrak{p}$ is unramified in $E \iff e_i = 1 \; \forall i$.*
3. *We say that $\mathfrak{p}$ splits completely in $E \iff e_1 = f_i = 1 \; \forall i$.*

Galois Extensions

Now assume that E/F is a Galois extension. For a general field extension this means that it is algebraic (automatic in our case because it is finite) and if $Aut(E/F)$ = field automorphisms of E fixing F then $E^{Aut(E/F)} = F$. In this case we write $Gal(E/F) = Aut(E/F)$, the Galois group of E/F. Clearly $Gal(E/F)$ preserves $\mathcal{O}_E$. It is a standard result from basic Galois theory that if E/F is finite then $[E : F] = |Gal(E/F)|$.

Let $\mathfrak{P} \subset \mathcal{O}_E$ be a prime ideal and $\sigma \in Gal(E/F)$. We denote by $\sigma\mathfrak{P} \subset \mathcal{O}_E$ the image of $\mathfrak{P}$ under σ. It is elementary to show that $\sigma\mathfrak{P}$ is a prime ideal and if $\mathfrak{p} \subset \mathcal{O}_F$ is a prime ideal such that $\mathfrak{P}|\mathfrak{p}\mathcal{O}_E$ then $\sigma\mathfrak{P}|\mathfrak{p}\mathcal{O}_E$. It is clear also that $e(\mathfrak{P}/\mathfrak{p}) = e(\sigma\mathfrak{P}/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{p}) = f(\sigma\mathfrak{P}/\mathfrak{p})$

Proposition. *Let E/F be a Galois extension of number fields. Let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal. Then $Gal(E/F)$ acts transitively on the primes dividing $\mathfrak{p}$.*

Proof. This is proposition 2 of §10 of the Local Fields chapter of Cassels/Frohlich. □

Corollary. *Let E/F be a Galois extension of number fields. Let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal. If $\mathfrak{P} \subset \mathcal{O}_E$ is a prime ideal dividing $\mathfrak{p}\mathcal{O}_E$ then it's ramification index and residue class degree only depend on $\mathfrak{p}$.*

Ramification, Traces and Norms

Let E/F be a finite extension of number fields. Given $x \in E$ there is a natural F-linear maps of vector spaces:

$$\begin{aligned} \phi_x : E &\longrightarrow E \\ y &\longrightarrow xy \end{aligned}$$

Thinking about this as a map of finite dimensional F-vector spaces we may compute it's trace and determinant:

Definition. *1. We define the Trace map of E/F by:*

$$\begin{aligned} Tr_{E/F} : E &\longrightarrow F \\ x &\longrightarrow trace(\phi_x) \end{aligned}$$

2. We define the Norm map of E/F by:

$$\begin{aligned} N_{E/F} : E &\longrightarrow F \\ x &\longrightarrow det(\phi_x) \end{aligned}$$

It is easy to show that $Tr_{E/F}(\mathcal{O}_E) \subset \mathcal{O}_F$ and $N_{E/F}(\mathcal{O}_E) \subset \mathcal{O}_F$

Proposition. *The trace map defines a non-degenerate, symmetric F-bilinear form:*

$$\begin{aligned} B : E \times E &\longrightarrow F \\ (u, v) &\longrightarrow Tr_{E/F}(uv). \end{aligned}$$

Proof. This is in proposition 1 of §4 of the Local Fields chapter of Cassels/Frohlich. It is a general fact about finite separable field extensions. □

Definition. *Let $\{x_1, ...x_n\} \subset E$ be an F-basis. We define $\Delta(x_1, ..., x_n) = det(B(x_i, x_j))$.*

We see that $\{x_1, ...x_n\} \subset \mathcal{O}_E \Rightarrow \Delta(x_1, ..., x_n) \in \mathcal{O}_F$.

Definition. *We define the relative discriminant of E/F, $\mathfrak{D}(E/F) \subset \mathcal{O}_F$ as the ideal generated by all $\Delta(x_1, ..., x_n)$, where $\{x_1, ...x_n\} \subset \mathcal{O}_E$ are an F-basis for E.*

Key Property of Relative Discriminant:

Theorem. *Let E/F be an extension of number fields. Let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal. The $\mathfrak{p}$ ramifies in $E \iff \mathfrak{p} | \mathfrak{D}(E/F)$.*

Proof. This is Corollary 1 of §5 of the Local Fields chapter of Cassels/Frohlich. □

Corollary. *Let E/F be a finite extension of number fields. All but finitely many prime ideals $\mathfrak{p} \subset \mathcal{O}_F$ are unramified in E.*

Proof. By the previous theorem we know that a prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ ramifies in $F \iff \mathfrak{p} | \mathfrak{D}(E/F)$. But $\mathcal{O}_F$ is a Dedekind domain, hence only finitely many primes ideal can divide $\mathfrak{D}(E/F)$. □

The Artin Map

Let E/F be a Galois extension of number fields, $\mathfrak{p} \subset \mathcal{O}_F$ a prime ideal. Let us assume that $\mathfrak{p}\mathcal{O}_E$ splits into prime ideals in $\mathcal{O}_E$ as above. We know that in this situation all the e_i are equal and all the f_i are equal. We will denote their common value by $e(\mathfrak{p})$ and $f(\mathfrak{p})$ respectively. Combining several of the above results we know that

$$|Gal(E/F)| = [E : F] = m \times e(\mathfrak{p}) \times f(\mathfrak{p}).$$

Let $\mathfrak{P} \subset \mathcal{O}_E$ be one of the primes dividing $\mathfrak{p}\mathcal{O}_E$.

Definition. *The decomposition group at $\mathfrak{P}$ is*

$$G(\mathfrak{P}) := \{\sigma \in Gal(E/F) | \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Viewing $Gal(E/F)$ as a finite group acting on the set of primes dividing $\mathfrak{p}$ this is clearly the stabiliser group of $\mathfrak{P}$. Recall that $Gal(E/F)$ preserves $\mathcal{O}_E$ (and trivially fixes $\mathcal{O}_F$). Hence if $\sigma \in Gal(\mathfrak{P})$ then it naturally gives rise to a field automorphism of $\mathbb{F}_{\mathfrak{P}}$ which fixes $\mathbb{F}_{\mathfrak{p}}$. $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is an extension of finite fields, and is consequently Galois. Hence we get a natural map homomorphism of groups:

$$\eta : G(\mathfrak{P}) \longrightarrow Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

Proposition. *η is surjective.*

Proof. This is proposition 14 of §5 of Chapter 1 of Algebraic Number Theory by Serge Lang. □

Number Theory

Alexander Paulin

September 10, 2009

Lecture 4

Let E/F be a Galois extension of number fields, with Galois group $Gal(E/F)$. Let $\mathfrak{p} \subset \mathcal{O}_F$ be a non-zero prime ideal. We have the non-zero prime factorisation (in $\mathcal{O}_E$)

$$\mathfrak{p}\mathcal{O}_E = \mathfrak{P}_1^e....\mathfrak{P}_m^e,$$

where $e = e(\mathfrak{p})$, the ramification index. All the exponents are equal because the extension is Galois. Recall that for almost all such $\mathfrak{p}$, $e(\mathfrak{p}) = 1$. Similary the residue class degrees of each $\mathfrak{P}_i$ over $\mathfrak{p}$ are all equal and we denote their common value by $f(\mathfrak{p})$. We know from lecture 3 that

$$|Gal(E/F)| = [E : F] = m \times e(\mathfrak{p}) \times f(\mathfrak{p}).$$

Let $\mathfrak{P} = \mathfrak{P}_i$ for some $i \in \{1, ..., m\}$. Recall that decomposition group at $\mathfrak{P}$ is

$$G(\mathfrak{P}) := \{\sigma \in Gal(E/F) | \sigma\mathfrak{P} = \mathfrak{P}\}.$$

The action $Gal(E/F)$ on the primes dividing $\mathfrak{p}$ is transitive. Thinking about $Gal(E/F)$ as a finite group acting on the set of m primes dividing $\mathfrak{p}$, we see by the orbit-stabiliser theorem that $|G(\mathfrak{P})| = e(\mathfrak{p}) \times f(\mathfrak{p})$.

We also observed that there was naturally a homomorphism

$$\eta : G(\mathfrak{P}) \longrightarrow Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}),$$

which was in fact surjective.

Definition. *The kernel of η, denoted $T(\mathfrak{P})$, is the inertia subgroup of $Gal(E/F)$ at $\mathfrak{P}$.*

Proposition. $|T(\mathfrak{P})| = e(\mathfrak{p})$.

Proof. We know that $|Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})| = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}] = f(\mathfrak{p})$. Because η is surjective and $|G(\mathfrak{P})| = e(\mathfrak{p}) \times f(\mathfrak{p})$ we deduce from the 1st isomorphism theorem that $|T(\mathfrak{P})| = e(\mathfrak{p})$.

□

Hence for almost all non-zero primes $\mathfrak{p} \subset \mathcal{O}_F$ (i.e. those not dividing $\mathfrak{D}(E/F)$) we know that $G(\mathfrak{P}) \cong Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ for every non-zero prime $\mathfrak{P} \subset \mathcal{O}_E$ dividing $\mathfrak{p}$.

Interlude on Galois Theory for Extensions of Finite Fields

Let $\mathbb{F}$ be a finite field. Because it is finite we know that $char(\mathbb{F}) = p$ for some prime $p \in \mathbb{Z}$. This tells us that $\mathbb{F}_p \subset \mathbb{F}$ and consequently $|\mathbb{F}| = p^n = q$, for some $n \in \mathbb{N}$. Recall that any finite multiplicative subgroup of a field is cyclic. Hence $\mathbb{F}^*$ is cylic of order $q-1$. In particular no element has multiplicative order p.

Recall that on any ring of characteristic p there is a canonical endomorphism called the absolute frobenius, $Frob_p : x \to x^p$. We say that a ring of characteristic p is *perfect* if $Frob_p$ is an automorphism. By the above remarks it is clear that $\mathbb{F}$ is perfect.

It is a well known fact that $\mathbb{F}$ is uniquely determined up to isomorphism by its cardinality. Hence we may write $\mathbb{F} = \mathbb{F}_q$ without any ambiguity. Conversely, given any $q = p^n$ for $n \in \mathbb{N}$ there exists a finite field of order q. If $q = p^n$ and $r = p^m$ such that $n|m \Rightarrow \mathbb{F}_q \subset \mathbb{F}_r$. In this case $\mathbb{F}_r/\mathbb{F}_q$ is finite and Galois. There is a canonical Frobenius element $Frob_q = (Frob_p)^n \in Gal(\mathbb{F}_r/\mathbb{F}_q)$, which acts on $\mathbb{F}_r$ by $Frob_q : x \to x^q$. This element naturally generates $Gal(\mathbb{F}_r/\mathbb{F}_q)$, and we deduce that it is cyclic.

All of these facts can be found in any elementary textbook on Galois Theory.

Back to the Artin Map

Keeping the above notation let us assume that $e(\mathfrak{p}) = 1$. Hence $\eta : G(\mathfrak{P}) \to Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is an isomorphism. Let $Frob_{\mathfrak{P}} \in Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$, be the Frobenius.

Definition. *The Frobenius element at $\mathfrak{P}$ is*

$$(E/F, \mathfrak{P}) := \eta^{-1}(Frob_{\mathfrak{P}}) \in G(\mathfrak{P}) \subset Gal(E/F)$$

If $K/E/F$ is a tower of number fields, all extension being Galois, then there is a natural restriction homomorphism :

$$res_E : Gal(K/F) \longrightarrow Gal(E/F).$$

If $\mathcal{P} \subset \mathcal{O}_K$ is a non-zero prime ideal lying over $\mathfrak{P} \subset \mathcal{O}_E$ then it is not hard to show that

$$res_E((K/F, \mathcal{P})) = (E/F, \mathfrak{P}).$$

In his sense the Frobenius respects field extensions.

Let F be a field and $\bar{F}$ denote an algebraic closure of F. It is a standard fact that $\bar{F}$ is unique up to isomorphism. By the fundamental theorem of algebra, if F is a number field we may naturally consider $\bar{F} \subset \mathbb{C}$. In this case, because $F/\mathbb{Q}$ is finite (hence algebraic) we may identify $\bar{F}$ and $\bar{\mathbb{Q}}$. Here $\bar{F}/F$ is not finite, because of the existence of irreducible polynomials over $\mathbb{Q}$ of arbitrary degree.

Definition. *Let E/F and K/F be two extensions of F contained in $\bar{F}$. The compositum of E and K, denoted by EK, is the minimal subfield of $\bar{F}$ containing E and F.*

Let us now restrict to the case where E, F and K are number fields. Furthermore let us assume that E/F and K/F are both Galois. It is not hard to show that EK/F is a Galois extension and there is a natural injective homorphism:

$$\begin{aligned} \phi : Gal(EK/F) &\longrightarrow Gal(E/F) \times Gal(K/F) \\ \sigma &\longrightarrow (res_E(\sigma), res_K(\sigma)) \end{aligned}$$

In general ϕ is not an isomorphism, except in the case when $E \cap K = F$. If $\mathsf{P} \subset \mathcal{O}_{EK}$ is a non-zero rime ideal lying over $\mathcal{P} \subset \mathcal{O}_K$ and $\mathfrak{P} \subset \mathcal{O}_E$ then it is true that:

$$\phi((EK/F, \mathsf{P})) = ((E/F, \mathfrak{P}), (K/F, \mathcal{P})).$$

In this sense the Frobenius element respects composition of fields.

Let $\sigma \in Gal(E/F)$. Then $G(\sigma\mathfrak{P}) = \sigma G(\mathfrak{P})\sigma^{-1}$. Consequently $(E/F, \sigma\mathfrak{P}) = \sigma(E/F, \mathfrak{P})\sigma^{-1}$. Hence, in general there is no canonical way of associating a Frobenius element to a non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$. Instead we have:

Definition. *Let $\mathfrak{p} \subset \mathcal{O}_F$ be a non-zero prime ideal and $\mathfrak{P} \subset \mathcal{O}_E$ a non-zero prime ideal lying over $\mathfrak{p}$. We define the Frobenius class at $\mathfrak{p}$ to be the conjugacy class*

$$Frob_{\mathfrak{p}} := \{\sigma(E/F, \mathfrak{P})\sigma^{-1} | \sigma \in Gal(E/F)\} \subset Gal(E/F)\}.$$

Because $Gal(E/F)$ acts transitively on the primes lying over $\mathfrak{p}$ and the previous comment this is well defined. Observe that $Frob_{\mathfrak{p}} = \{1\} \iff \mathfrak{p}$ splits completely in E.

We say that E/F is Abelian if $Gal(E/F)$ is an Abelian group. This is a *very* restrictive property. Global Class Field Theory gives a way of classifying such extensions. It crucially relies on the fact that in this case $Frob_{\mathfrak{p}}$ is a well defined element of $Gal(E/F)$. We will return to this once we have introduced the important concept of a local field.

Tchebotarev Density Theorem. *Let E/F be Galois extension of number fields. Let $C \subset Gal(E/F)$ be a conjugacy class. Then the primes $\mathfrak{p} \subset \mathcal{O}_F$ such that $Frob_{\mathfrak{p}} = C$ have density $|C|/|Gal(E/F)|$ in the set of all non-zero prime ideals. In particular there are infinitely many such primes.*

Remarks. *1. By density we mean density in the sense of Dirichlet, i.e. If $F = \mathbb{Q}$ then the density of S, a subset of the primes numbers equals the limit as n tends to ∞ of*

(Number of elements of S less than n) / (Number of primes less than n).

2. This theorem is deep because it exhibits a link between the distribution of the primes and their algebraic behaviour.

Theorem. *Let E/F and K/F be two Galois extensions of number fields (thought of as both lying in a fixed algebraic closure $\bar{F}$). Let $Spl(E/F)$ and $Spl(K/F)$ denote the subset of non-zero prime ideals in $\mathcal{O}_F$ which split completely in E and K respectively. Then*

$$E \subset K \iff Spl(K/F) \subset Spl(E/F).$$

Proof. If $E \subset K$ we know by the multiplicative behavior of ramification index and residue class degree in towers of extensions that $Spl(K/F) \subset Spl(E/F)$. Let us assume that $Spl(K/F) \subset Spl(E/F)$. Let $\mathfrak{p} \subset \mathcal{O}_F$ be a non-zero prime ideal. Observe that because Frobenius respects composition of fields

$$\mathfrak{p} \text{ splits completely in } EK \iff \mathfrak{p} \text{ splits completely in both } E \text{ and } K.$$

Hence in general we have $Spl(EK/F) = Spl(E/F) \cap Spl(K/F)$. We deduce that

$$Spl(K/F) \subset Spl(E/F) \Rightarrow Spl(EK/F) = Spl(K/F).$$

By the Tchebotarev density theorem we deduce that $[EK : F] = [K : F] \Rightarrow E \subset K$. □

Hence number fields which are Galois over $\mathbb{Q}$ are determined (up to isomorphism) by the primes in $\mathbb{Z}$ which split completely. Let me give you another powerful consequence of the density theorem.

Crash Course on Cyclotomic Fields

Let $n \in \mathbb{N}$. Fix $\zeta_n \in \mathbb{C}$, a primitive *nth* root of unity. We denote by $\mathbb{Q}(\zeta_n)$, the splitting field of $f(x) = x^n - 1$. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is finite and Galois. If $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ then $\sigma(\zeta_n)$ is again a primitive *nth* root of unity. This establishes an isomorphism

$$\chi : Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*,$$

where $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$. Hence $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an Abelian extension. It can be shown that a prime $p \in \mathbb{Z}$ ramifies in $\mathbb{Q}(\zeta_n)$ if and only if $p|n$. Note that because $\mathbb{Z}$ is a PID we can freely switch between the concept of an ideal and a positive integer. Hence given $p \in \mathbb{Z}$ coprime to n we get a canonical element $Frob_p \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Proposition. $Frob_p(\zeta_n) = \zeta_n^p$

Proof. This is the proposition in §3.4 of Tate's article on Global Class Field Theory in Cassels/Frohlich. □

Dirichlet's Theorem on Arithmetic Progressions. *Let $a \subset \mathbb{Z}$ be coprime to n. Then the arithmetic progression $S = \{a + kn | k \in \mathbb{N}\}$ contains infinitely many primes.*

Proof. Because a is coprime to n is defines a unique element of $(\mathbb{Z}/n\mathbb{Z})^*$, which we denote by $[a]$. By the Tchebotarev density theorem the know that there exist infinitely many primes $p \in \mathbb{Z}$ such that $\chi(Frob_p) = [a]$. But by the previous proposition we know that this occurs precisely when a and p are congruent modulo n. Hence there are infinitely many such primes. □

The Tchebotarev density theorem is a vast generalization of this result.

Number Theory

Alexander Paulin

September 15, 2009

Lecture 5

Local Fields

The rational numbers come equipped with a canonic metric: For $x, y \in \mathbb{Q}$ we define $d(x, y) := |x - y|$, where $|.|$ denotes the standard absolute value. Completion of $\mathbb{Q}$ with respect to this metric gives $\mathbb{R}$. $\mathbb{R}$ inherits a canonical metric and is complete with respect to it. Heuristically we see that to truly *understand* $\mathbb{Q}$ we much *understand* $\mathbb{R}$. Let us examine, in abstraction the process of completion.

Absolute Values and Valuations

Let F be a field.

Definition. *A discrete valuation is a function v: $F^* \longrightarrow \mathbb{Z}$, such that*

1. *$v(xy) = v(x) + v(y) \ \ \forall x, y \in F^*$*
2. *$v(x + y) \geq min\{v(x), v(y)\} \ \ \forall x, y \in F^*$*

Remarks. *The example we will be interested in is when F is a number field. In this case we know there is a natural homorphism:*

$$\begin{aligned} F^* &\longrightarrow \mathfrak{I}(\mathcal{O}_F) \\ x &\longrightarrow (x) \end{aligned}$$

The latter is the free abelian group on the set of non-zero prime ideals of $\mathcal{O}_F$. Hence for any non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ we get the valuation $v_\mathfrak{p}$ which sends $x \in F^*$ to the exponent of $\mathfrak{p}$ in the prime factorization of $(x) \in \mathfrak{I}(\mathcal{O}_F)$.

Definition. *A discrete valuation ring (DVR) is a PID with only one non-zero prime ideal. A domain R is a DVR $\iff$ $F = Frac(R)$ admits a discrete valuation, v such that*

$$R = \{x \in F^* | v(x) \geq 0\} \cup \{0\}.$$

Because a PID is always integrally closed we deduce that R is a DVR $\iff$ R is a Dedekind domain with exactly on non-zero prime ideal. Being a Dedekind domain is preserved under localisation at a prime ideal. Hence If R is a Dedekind domain, and $\mathfrak{p} \subset R$ is a non-zero prime ideal then $R_{\mathfrak{p}}$ is a DVR. Conversely, a Noetherian domain R which is not field is Dedekind $\iff$ for every non-zero maximal ideal $\mathfrak{p} \subset R$, $R_{\mathfrak{p}}$ is a DVR. All of these results are very standard and can be found in *An Introduction to Commutative Algebra* by Atiyah and Macdonald.

Definition. *Let F be a field. An absolute value on F is a function $|.| : F \longrightarrow \mathbb{R}_+$ such that:*

1. $|x| = 0 \iff x = 0$.
2. $\forall x, y \in F \; |xy| = |x| \times |y|$.
3. $\forall x, y \in F \; |x + y| \leq |x| + |y|$.

These conditions force $|1|^2 = |1|$, so $|1| = 1$. Similarly $|-1| = 1$ Hence $|1/x| = 1/|x|$ and $|-x| = |x|$ for all $x \in F^*$. The canonical example of a field with an absolute value is any subfield of $\mathbb{C}$ together with the usual absolute value.

If $(F, |.|)$ is a field with an absolute value then we may canonically define a metric on F: for $x, y \in F$ $d(x, y) := |x - y|$. We may define the trivial absolute value on a field by $|x| = 1 \; \forall x \in F^*$. In general we will be interested in non-trivial absolute values. The resulting topology on F makes it a topological field.

Let (F, v) be a Field together with a discrete valuation. Fix $c \in (0, 1)$. We may define the absolute value $|.|_{v,c}$ on F by

$$\begin{array}{rccc} |.|_{v,c} : & F & \longrightarrow & \mathbb{R}_+ \\ & x & \longrightarrow & c^{v(x)} \end{array}$$

Strictly speaking this function is not defined at zero so we set $|0|_{v,c} = 0$.

Theorem. *Let $|.|$ and $|.|'$ be two absolute values on a field F. Then they induce the same topology on F $\iff$ there exists $e > 0$ such that $|.|' = |.|^e$.*

Proof. This is the second lemma of §4 of the Global Fields Chapter of Cassels/Frohlich. □

We call two such absolute values equivalent. We deduce from this result that if (F, v) is a field with discrete valuation then the topology defined above by the absolute value is independent of the choice of c.

Definition. *Let $(F, |.|)$ be field together with an absolute value. We say that $|.|$ is non-archimedean if the ultrametric triangle inequality holds:*

$$\forall x, y \in F \; |x + y| \leq max\{|x|, |y|\}.$$

If this does not hold we say that $|.|$ is archimedean.

This is a very strong condition. For example, it forces $|k| \leq 1$ for all $k \in \mathbb{Z}$. Any absolute value coming from a discrete valuation is non-archimedean. If $|.|$ is a non-archimedean absolute value on F then all equivalent absolute values are non-archimedean.

Theorem. *Any field F with an archimedean absolute value is isomorphic to a subfield of $\mathbb{C}$, the absolute value being equivalent to the one induced by the absolute value on $\mathbb{C}$.*

Proof. See pages 45 and 67 of *The Theory of Algebraic Numbers* by E. Artin. □

So fields with archimedean absolute values are familiar objects. Let us now focus on the non-archimedean case.

Let $(F, |.|)$ be a field together with a non-archimedean absolute value. Let $a \in F$ and $r \in \mathbb{R}$ $r > 0$. The closed ball of radius r around a defined to be

$$\bar{B}_r(a) := \{x \in F | |x - a| \leq r\}.$$

Let $b \in \bar{B}_r(a)$. Consider the open ball of radius $r/2$ around b,

$$B_{r/2}(b) := \{x \in F | |x - b| < r/2\}.$$

Observe that if $c \in B_{r/2}(a)$ then

$$|c - a| = |(c - b) + (b - a)| \leq max\{|c - b|, |b - a|\} \leq r.$$

Hence $B_{r/2}(b) \subset \bar{B}_r(a)$. We deduce that $\bar{B}_r(a)$ is in fact open! A similar argument shows that all *triangles* in F are isosceles!

Definition. *A topological space is totally disconnected if the only non-empty connected subsets are one point sets.*

Theorem. *Let $(F, |.|)$ be a field with a non-archimedean absolute value. Then F is totally disconnected under the induced topology.*

Proof. Let $X \subset F$ be a connected subset having two distinct points $x_0, x_1 \in X$. Choose $r > 0$ such that $r < |x_0 - x_1|$. We have a disjoint union

$$X = (X \cap \{|x - x_o| \leq r\}) \cap (X \cap \{|x - x_o| r\})$$

By the above we know that each piece is open (the the subset topology) in X. Note that each piece is non-empty as x_0 is in the first and x_1 is in the second. This contradicts the assumption that X is connected. □

Hence the topology in the non-archimedean case is wildly different than in the archimedean case.

Observe that in the non-archimedean setting $R = \{x \in F | |x| \leq 1\}$ is a subring. Similarly $M = \{x \in F | |x| < 1\}$ is an ideal. It is clear by the muliplicative behavior of $|.|$ that $a \in R^* \iff |a| = 1$. We deduce that R is a local ring with M as its unique maximal ideal. Both of these only depend on $|.|$ up to equivalence. Hence we may associate to F a residue field R/M.

Back to Number Fields

Let F be a number field. We saw that any non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ gives rise to a valuation on F. Hence by the above it gives an equivalence class of non-archimedean absolute values. Let $N(\mathfrak{p}) = |\mathbb{F}_\mathfrak{p}|$. We normalise the absolute value so that $|x|_\mathfrak{p} = (N(\mathfrak{p}))^{-v_\mathfrak{p}(x)}$ for all $x \in F^*$. In this case, R is the localisation of $\mathcal{O}_F$ at $\mathfrak{p}$ and the residue field is just $\mathbb{F}_\mathfrak{p}$.

Also observe that given $\sigma : F \longrightarrow \mathbb{C}$ an embedding we get an induced absolute value $|x|_\sigma = |\sigma(x)|$. This gives an example of an archimedean absolute value on F. It is a fact that there are precisely $[F : \mathbb{Q}]$ distinct such embeddings.

Fundamental Fact:

Theorem. *Let $F/\mathbb{Q}$ be a number field. Every non-trivial non-archimedean absolute value on F is equivalent to $|.|_\mathfrak{p}$ for a unique non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$. Up to equivalence, every archimedean absolute value of F is induced by an embedding $\sigma : F \longrightarrow \mathbb{C}$, and two such embedding give rise to equivalent absolute values if and only if they coincide or differ by complex conjugation.*

Proof. In the case $F = \mathbb{Q}$ this is a famous theorem of Ostrowski. The general case can be deduced from that. □

Definition. *Let F be a number field. By a place of F we mean an equivalence class of a non-trivial absolute value on F. We denote a place by v.*

By the above the places are indexed by non-zero prime ideals of $\mathcal{O}_F$ and embeddings $\sigma : F \longrightarrow \mathbb{C}$ up to complex conjugation. We call the non-archimedean places finite and the archimedean ones infinite.

If $\sigma : F \longrightarrow \mathbb{C}$ is an embedding then we say that it is a real embedding if it's image is contained in $\mathbb{R}$. If not then we say it is complex.

The following important result links the infinite and finite places:

Theorem. *Let F be a number field. For $x \in F^*$*

$$\prod_{v|\infty} |x|_v^{e(v)} \cdot \prod_{v \text{ finite}} |x|_v = 1.$$

Where $e(v) = 1$ if v comes from a real embedding and $e(v) = 2$ is v comes from a complex embedding.

Proof. This is the Theorem in §12 of the chapter on Global Fields in Cassels/Frohlich. □

Number Theory

Alexander Paulin

September 21, 2009

Lecture 6

There is a very strong analogy between the above and the theory of smooth projective algebraic curves over $\mathbb{C}$ (or any algebraically closed field). Let X be such a curve and $x \in X$ be a closed point. Being smooth at x is equivalent to the stalk of functions at x, denoted $\mathcal{O}_{X,x}$, being regular local ring of dimension 1. This is equivalent to being a DVR. Hence $Frac(\mathcal{O}_{X,x})$ is a field together with a discrete valuation. Intuitively this is the order of vanishing of a meromorphic function at x. The natural embedding $K_X \longrightarrow Frac(\mathcal{O}_{X,x})$, induces a discrete valuation on K_X. Hence as above, for every such x, we get an equivalence class of absolute values on K_X. As above this gives all non-trivial places on K_X, one for each closed point. There is an equivalence between transcendence degree one field extensions of $\mathbb{C}$ and smooth projective algebraic curves over $\mathbb{C}$. Hence we may define an *abstract* algebraic curve over $\mathbb{C}$ as a transcendence degree one field extension of $\mathbb{C}$ together with it's non-trivial places. This definition is given in §1 of Hartshorne. Observe that unlike the number field case all places are non-archimedean. This makes this theory, although analogous, fundamentally easier.

Completions

Given an absolute value $|.|$ on a field F, we may naturally complete F with respect to $|.|$. We denote the completion by $\hat{F}$. Recall that $\hat{F}$ is the set of Cauchy sequences, modulo null sequences. Observe that the process of completion preserves the algebraic structure, in particular $\hat{F}$ is again a field. By the completeness of $\mathbb{R}$, $\hat{F}$ inherits an absolute value, which we also denote by $|.|$. It is a simple exercise to show that $(\hat{F}, |.|)$ is complete.

Proposition. *Let $(F, |.|)$ be a field together with an archimedean absolute value. Then $\hat{F}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ and the absolute value is equivalent to the standard one in each case.*

Proof. By a previous theorem we know that F is isomorphism to a subfield of $\mathbb{C}$, and with respect to this embedding $|.|$ is equivalent to the standard absolute value. Let us denote this embedding by ϕ. If ϕ is a real embedding then because $\mathbb{Q} \subset F$ we deduce that $\hat{F}$ is isomorphic to $\mathbb{R}$, and the induced absolute value is equivalent to the standard one. If

ϕ is complex then the completion must isomorphic $\mathbb{C}$, and the induced absolute value is equivalent to the standard one. $\square$

Hence up to equivalence the only complete archimedean fields are $\mathbb{R}$ and $\mathbb{C}$, together with their usual absolute values. The situation in the non-archimedean case is radically different.

Proposition. *Let $(F, |.|)$ be a field together with a non-archimedean absolute value. Then $|\hat{F}| = |F| \subset \mathbb{R}_+$.*

Proof. Let $a = (a_n)_{n\in\mathbb{N}} \in \hat{F}$ be a Cauchy sequence in F. Then $(|a_n|)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{R}_+$. By definition $|a|$ is the limit of this sequence. Assume that $l = |a| \neq 0$. Hence $\exists N \in \mathbb{N}$ such that $|a_n| > l/2$ and $|a_n - a_m| < l/2 \; \forall n, m > N$. By the non-archimedean property we know that $|a_n - a_m| \leq \max\{|a_n|, |a_m|\}$ and that if $|a_n|$ and $|a_m|$ are distinct then equality must hold. By our choice of N, we deduce that $|a_n| = |a_m| \; \forall n, m > N$. Hence $|a_n| = l \; \forall n > N$. $\square$

Hence if $|.|$ is an absolute value coming from a discrete valuation then $|\hat{F}^*| \subset \mathbb{R}_+$ is a discrete subset. Also observe that the inherited absolute value is again non-archimedean.

Proposition. *Let $(F, |.|)$ be a field together with a non-archimedean absolute value. Let $\hat{F}$ be the completion. Then the residue field of F is isomorphic to the residue field of $\hat{F}$.*

Proof. Let $\mathbb{F}$ and $\hat{\mathbb{F}}$ be the reside fields of F and $\hat{F}$ respectively. There is clearly an embedding $\phi : \mathbb{F} \longrightarrow \hat{\mathbb{F}}$. Observe that if $\bar{a} \in \hat{\mathbb{F}}^*$ then it has a representative $a = (a_n)_{n\in\mathbb{N}} \in \hat{F}$ such that $|a| = 1$. This implies $\exists N \in \mathbb{N}$ such that $|a_n| = 1$ and $|a_n - a_m| < 1/2 \; \forall n > N$. Let $\bar{a}_{N+1} \in \mathbb{F}$ be the element of the residue field given by a_{N+1}. Then $\phi(\bar{a}_{N+1}) = \bar{a}$, and we deduce that ϕ is surjective and hence an isomorphism. $\square$

Here are two general facts about complete fields:

Theorem. *Let $(F, |.|)$ be a field together with an absolute value. Assume further that F is complete. Let E/F be an algebraic extension. Then there is a unique absolute value on E extending that on F. If E/F is finite then with respect to this absolute value E is complete.*

Proof. This is the theorem in §10 of the Global Fields Chapter of Cassels/Frohlich $\square$

Theorem. *Let $(F, |.|)$ be a field together with two non-trival non-archimedean absolute values $|.|$ and $|.|'$. Assume furthermore that F is complete with respect to both. Then $|.|$ and $|.|'$ are equivalent.*

Proof. This can be found on page 104 of Frohlich/Taylor. $\square$

Definition. *Let $(F, |.|)$ be a field together with a non-archimedean absolute value. Assume further that $|.|$ is induced by a discrete valuation, that F is complete and that the residue field is of finite cardinality $q \in \mathbb{N}$. Then we say that F is a* ***non-archimedean local field****.*

Some authors have a slightly more general definition, demanding only that the residue field be of finite characteristic and perfect. By an **archimedean local field** we mean a topological field topologically isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

Let F be a non-archimedean local field. Let $R \subset F$ be the valuation ring, with maximal ideal $m \subset R$. Then R is a DVR and hence m is principal. Fix $\pi \in m$ such that $(\pi) = m$. Observe that $|\pi| < 1$ and that $|x| \leq |\pi| \ \forall x \in m$. Hence $|\pi|$ maximal for in the set $\{|x| \in \mathbb{R}_+ \ | x \in m\}$. We deduce that all $\alpha \in R$ can be written uniquely in the form $\alpha = \pi^e \epsilon$, for e a positive integer and $\epsilon \in R^*$. Observe π is unique up to multiplication by a unit in R.

Proposition. *Every element $\alpha \in R$ can be written uniquely in the form*

$$\alpha = \sum_{n=0}^{\infty} a_n \pi^n,$$

where the a_n run through some fixed set Σ of representatives in R of R/m.

Proof. There is a uniquely defined $a_0 \in \Sigma$ such that $|\alpha - a_0| < 1$. Then $\alpha_1 = \pi^{-1}(\alpha - a_0) \in R$. Now define $a_1 \in \Sigma$ by $|\alpha_1 - a_1| < 1$. And so on.

□

Corollary. *Every $\alpha \in F$ can be written uniquely in the form*

$$\alpha = \sum_{n=e}^{\infty} a_n \pi^n,$$

where $e \in \mathbb{Z}$ and $a_j \notin m$. Moreover $|\alpha| = |\pi|^e$.

Proof. By the above we know that there exists a unique $e \in \mathbb{Z}$ such that $\alpha = \pi^e \epsilon$, where $\epsilon \in R^*$. By the above proof we know that we may expand ϵ as a power series in π with coefficients in Σ and that the leading term in this expansion is not in m. Multiplying this power series by π^e yields the result. □

One should think about this as a *decimal* expansion. The concept is totally analogous. Because Σ is finite we see that K has the same cardinality as $\mathbb{R}$.

Observe that R is the disjoint union of q open balls of radius 1. Each of these is in turn the disjoint union of q open ball of radius $|\pi|$. By induction we see that for $n \in \mathbb{N}$, R is the disjoint union of q^n disjoint open balls of radius $|\pi|^{n-1}$. The topology is completely different to the standards one on $\mathbb{R}$ (or indeed $\mathbb{C}$).

Observe also that R is *algebraically complete* with respect to m, i.e. the natural ring homomorphism $R \longrightarrow \varprojlim_{n \in \mathbb{N}} R/m^n R$ is an isomorphism. Furthermore it is a homeomorphism for the product topology on the projective limit after giving each $R/m^n R$ the discrete topology. By our assumption on the finiteness of the residue field each $R/m^n R$ is finite. Hence by Tychonoff's theorem R is compact. Hence we deduce

Theorem. *Let F be a non-archimedean local field. Then F is locally compact.*

Proof. Let $a \in F$, $r \in \mathbb{R}$ $r > 0$. F is a topological field, hence the closed ball $\bar{B}_r(a)$ is homeomorphic to R. We deduce that $\bar{B}_r(a)$ is compact. Thus there is a neighborhood of a which is compact. □

Note that both $\mathbb{R}$ and $\mathbb{C}$ are locally compact for the same reason - closed balls are compact.

Proposition. *Let F be a non-archimedean local field. If we give F^* the subspace topology, the it is a locally compact topological group.*

Proof. By the above we know that F^* is locally compact in the subspace topology. It is clearly a topological group as multiplication and taking reciprocals are continuous. □

In a moment we shall see examples of topological rings where the multiplicative group of units is **not** a topological group under the induced subspace topology. The reason that this result is important is that locally compact topological groups admit a unique (up to scalar) left (and right) Haar measure. Consequently we'll be able to introduce the full power of measure theory into our study.

Extensions of Non-Archimedean Fields

Let R be a discrete valuation ring of characteristic zero, which is complete with respect to the induced topology. Let $F = Frac(R)$. Fix a representative of the equivalence class of absolute values on F. R is the valuation ring of F. Let E/F be a finite extension of complete non-archimedean fields such that the restriction of the absolute value on E to F, equals the one on F. Recall that by completeness this uniquely determines the absolute value on E. Conversely, if F is a non-archimdean field and E/F is a finite extension, then there is a unique complete absolute value on E extending that on F

Recall that a DVR is a Dedekind domain with one non-zero prime ideal. Let $S \subset E$ is the integral closure R in E. By the abstract algebraic properties of Dedekind domains we know that that S is a Dedekind domain and is a free R-module of rank $[E : F]$. Moreover it must be a have only finitely many non-zero prime ideals and is hence a DVR. It is a fact that S is the valuation ring of E with respect to the absolute value. Let $\mathfrak{p} \subset R$ and $\mathfrak{P} \subset S$ be the non-zero prime ideals. We also know that

$$\mathfrak{p}S = \mathfrak{P}^e$$

for some $e \in \mathbb{N}$. We call this the ramification index of E/F and we denote it by $e(E/F)$.

If $\mathbb{F}_E$ and $\mathbb{F}_F$ are the respective finite residue fields we know that $\mathbb{F}_E$ is a finite field extension of $\mathbb{F}_F$. The degree of this extension is called the residue degree denoted $f(E/F)$.

Proposition. $[E : F] = e(E/F)f(E/F)$

Proof. This is proposition 3 of §5 of the chapter on Local fields in Cassels/Frohlich. □

Definition. *1. We say that E/F is unramified if $e(E/F) = 1$*

2. We say that E/F is totally ramified if $f(E/F) = 1$

3. We say that E/F tamely ramified if the characteristic of the residue fields does not divide $e(E/F)$.

4. We say that E/F is has wildly ramified if is not tamely ramified.

Now assume that E/F is Galois. Then $\mathbb{F}_E/\mathbb{F}_F$ is Galois and there is a natural group homomorphism

$$\phi : Gal(E/F) \longrightarrow Gal(\mathbb{F}_E/\mathbb{F}_F).$$

As in the number fields case this is surjective. We call $ker(\phi)$ the inertia subgroup, denoted $I_{E/F}$. Clearly $|I_{E/F}| = e(L/K)$. If E and F are local fields the residue fields are finite. Hence in this case E/F unramified $\Rightarrow$ ϕ is an isomorphism $\Rightarrow$ $Gal(E/F)$ is cyclic.

Back to Number Fields

Let F be a number field. Let v be a place of F, i.e an equivalence class of non-trivial absolute values on F. Because completion is a topological property we may form the completion of F at v in a well defined way to get the complete topological field F_v. There are two possible situations:

1. If v is archimedean then either F_v is $\mathbb{R}$ or $\mathbb{C}$ depending on whether the corresponding equivalence class of embedding $\phi : F \to \mathbb{C}$ is real or complex. Thus all archimedean completions are archimedean local fields

2. If v is non-archimedean then it corresponds to a non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ and we often write $F_\mathfrak{p} = F_v$. The discrete valuation ring will be denoted by $\mathcal{O}_{F_\mathfrak{p}}$ (or sometimes $\mathcal{O}_v$). Recall that the residue field is preserved by completion. Thus the residue field of $F_\mathfrak{p}$ is $\mathbb{F}_\mathfrak{p}$. Hence all non-archimedean completions are non-archimdean local fields.

Let $\mathcal{D}_F := \prod_v F_v$ be the direct product over all places. Giving $\mathcal{D}_F$ the product topology makes it a topological ring. We say that $x \in \mathcal{D}_F$ is *restricted* if for all but finitely many non-archimedean places v, $x_v \in \mathcal{O}_v$.

Definition. *Let F be a number field. The ring of Adeles of F, denoted $\mathbb{A}_F$ is the subring of $\mathcal{D}_F$ consisting of restricted element.*

Observe that $\mathbb{A}_F$ is a topological ring under the subspace topology. Because each of the completions F are locally compact, $\mathbb{A}_F$ is a locally compact topological ring. As we shall see ring is supremely important in the arithmetic theory of F. Incidentally, they are named after Serre's wife. The units of $\mathbb{A}_F$ are called the ideles. We may think of the ideles as the restricted tensor product over all F_v^* where for almost all places the entry is contained in

$\mathcal{O}_v^*$. We give the ideles of F the product topology. This makes the ideles of F a locally compact topological group. **Warning**: This is not the subspace topology. Under the subspace topology taking inverses is not continuous!

For $p \in \mathbb{N}$ a prime number the corresponding completion of $\mathbb{Q}$ is called the p-adic numbers and is denoted by $\mathbb{Q}_p$. We denote its valuation ring $\mathbb{Z}_p$, also called the p-adic integers. If F is a number field and the non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ lies over $(p) \subset \mathbb{Z}$ then $F_\mathfrak{p}$ is naturally a field extension of $\mathbb{Q}_p$. If F is a non-archimedean local field of characteristic zero and residue characteristic p then F is automatically a finite extension of $\mathbb{Q}_p$. It is a fact that all such local fields are isomorphic to ones coming from this global construction.

As above, the discrete valuation ring of $\mathcal{O}_{F_\mathfrak{p}} \subset F_\mathfrak{p}$ is the integral closure of $\mathbb{Z}_p$ in $F_\mathfrak{p}$. More generally, if E/F is an extension of number fields and $\mathfrak{P} \subset \mathcal{O}_E$ is a non-zero prime ideal lying over $\mathfrak{p} \subset \mathcal{O}_F$, then $E_\mathfrak{P}$ is naturally a finite extension of $F_\mathfrak{p}$ and $\mathcal{O}_{E_\mathfrak{P}}$ is the integral closure of $\mathcal{O}_{F_\mathfrak{p}}$ in $E_\mathfrak{P}$.

Recall that a DVR is a Dedekind domain with precisely one non-zero prime ideal. In this case the unique non-zero prime ideal is $\mathfrak{p}\mathcal{O}_{F_\mathfrak{p}}$, and we denote it by $\mathfrak{p}$ again. As above we know that

$$\mathfrak{p}\mathcal{O}_{E_\mathfrak{P}} = \mathfrak{P}^e$$

for $e = e(E_\mathfrak{P}/F_\mathfrak{p})$. It is a straight forward exercise to show that that in this setting $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$, so the local and global ramification indexes coinicide. If E/F is Galois then $E_\mathfrak{P}/f_\mathfrak{p}$ is Galois.

Proposition. *The Decomposition group at $\mathfrak{P}$, $G(\mathfrak{P}) \subset Gal(E/F)$, is isomorphic to $Gal(E_\mathfrak{P}/F_\mathfrak{p})$.*

Proof. This is proposition 3 of §10 of the chapter on local Fields in Cassel's/Frohlich. □

Number Theory

Alexander Paulin

October 25, 2010

Lecture 7

Extensions of Non-Archimedean Fields

Let R be a discrete valuation ring of characteristic zero, which is complete with respect to the induced topology. Furthermore let us assume that R has a perfect residue field of finite characteristic. Let $F = Frac(R)$. Fix a representative of the equivalence class of absolute values on F. R is the valuation ring of F. Let E/F be a finite extension of complete non-archimedean fields such that the restriction of the absolute value on E to F, equals the one on F. Recall that by completeness this uniquely determines the absolute value on E. Conversely, if F is a non-archimdean field and E/F is a finite extension, then there is a unique complete absolute value on E extending that on F

Recall that a DVR is a Dedekind domain with one non-zero prime ideal. Let $S \subset E$ be the integral closure R in E. By the abstract algebraic properties of Dedekind domains we know that that S is a Dedekind domain and is a free R-module of rank $[E : F]$. Moreover it must be a have only finitely many non-zero prime ideals and is hence a DVR. It is a fact that S is the valuation ring of E with respect to the absolute value. Let $\mathfrak{p} \subset R$ and $\mathfrak{P} \subset S$ be the non-zero prime ideals. We also know that

$$\mathfrak{p}S = \mathfrak{P}^e$$

for some $e \in \mathbb{N}$. We call this the ramification index of E/F and we denote it by $e(E/F)$.

If $\mathbb{F}_E$ and $\mathbb{F}_F$ are the respective finite residue fields we know that $\mathbb{F}_E$ is a finite field extension of $\mathbb{F}_F$. The degree of this extension is called the residue degree denoted $f(E/F)$.

Proposition. $[E : F] = e(E/F)f(E/F)$

Proof. This is proposition 3 of §5 of the chapter on Local fields in Cassels/Frohlich. □

Definition.

1. *We say that E/F is unramified if $e(E/F) = 1$*
2. *We say that E/F is totally ramified if $f(E/F) = 1$*
3. *We say that E/F tamely ramified if the characteristic of the residue fields does not divide $e(E/F)$.*

4. We say that E/F is wildly ramified if is not tamely ramified.

Now assume that E/F is Galois. Then $\mathbb{F}_E/\mathbb{F}_F$ is Galois and there is a natural group homomorphism

$$\phi : Gal(E/F) \longrightarrow Gal(\mathbb{F}_E/\mathbb{F}_F).$$

As in the number fields case this is surjective. We call $ker(\phi)$ the inertia subgroup, denoted $I_{E/F}$. Clearly $|I_{E/F}| = e(E/F)$. If E and F are local fields the residue fields are finite. Hence in this case E/F unramified $\Rightarrow \phi$ is an isomorphism $\Rightarrow Gal(E/F)$ is cyclic.

Back to Number Fields

Let F be a number field. Let v be a place of F, i.e an equivalence class of non-trivial absolute values on F. Because completion is a topological property we may form the completion of F at v in a well defined way to get the complete topological field F_v. There are two possible situations:

1. If v is archimedean then either F_v is $\mathbb{R}$ or $\mathbb{C}$ depending on whether the corresponding equivalence class of embedding $\phi : F \to \mathbb{C}$ is real or complex. Thus all archimedean completions are archimedean local fields

2. If v is non-archimedean then it corresponds to a non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ and we often write $F_{\mathfrak{p}} = F_v$. The discrete valuation ring will be denoted by $\mathcal{O}_{F_{\mathfrak{p}}}$ (or sometimes $\mathcal{O}_v$). Recall that the residue field is preserved by completion. Thus the residue field of $F_{\mathfrak{p}}$ is $\mathbb{F}_{\mathfrak{p}}$. Hence all non-archimedean completions are non-archimdean local fields.

Let $\mathcal{D}_F := \prod_v F_v$ be the direct product over all places. Giving $\mathcal{D}_F$ the product topology makes it a topological ring. We say that $x \in \mathcal{D}_F$ is *restricted* if for all but finitely many non-archimedean places v, $x_v \in \mathcal{O}_v$.

Definition. *Let F be a number field. The ring of Adeles of F, denoted $\mathbb{A}_F$ is the subring of $\mathcal{D}_F$ consisting of restricted element.*

We do **not** give $\mathbb{A}_F$ the subspace topology. Instead we define a basis of open subsets as follows: Let S be a finite subset of places including all archimedean places. For $v \in S$, let $U_v \subset F_v$ be an open subset. Then we define the subset

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v \subset \mathbb{A}_F,$$

to be open. Such sets subsets form the basis of a topology for $\mathbb{A}_F$. With respect to this topology $\mathbb{A}_F$ becomes a topological ring. This topology is not the subspace topology. We do this because each of the completions F are locally compact and $\mathcal{O}_v$ is compact for all non-archimedean places, hence this topology makes $\mathbb{A}_F$ is a locally compact topological ring. As we shall see, this ring is supremely important in the arithmetic theory of F. Incidentally, they are named after Serre's wife. We denote by $\mathbb{A}_F^{\infty}$ the restricted direct product over

the non-archimedean places only. Observe that there is a natural continuous injective map $F \longrightarrow \mathbb{A}_F$. The units of $\mathbb{A}_F$ are called the ideles. Clearly there is an embedding $F^* \longrightarrow \mathbb{A}_F^*$. We may think of the ideles as the restricted direct product over all F_v^* where for almost all places the entry is contained in $\mathcal{O}_v^*$. We do **not** give the ideles of F the obvious subspace topology. Instead we define a basis of open subsets as follows: Let S be a finite subset of places including all archimedean places. For $v \in S$, let $U_v \subset F_v^*$ be an open subset. Then we define the subset

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v^* \subset \mathbb{A}_F^*,$$

to be open. This makes the ideles of F a locally compact topological group.

For $p \in \mathbb{N}$ a prime number the corresponding completion of $\mathbb{Q}$ is called the p-adic numbers and is denoted by $\mathbb{Q}_p$. We denote its valuation ring $\mathbb{Z}_p$, also called the p-adic integers. If F is a number field and the non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ lies over $(p) \subset \mathbb{Z}$ then $F_\mathfrak{p}$ is naturally a field extension of $\mathbb{Q}_p$. If F is a non-archimedean local field of characteristic zero and residue characteristic p then F is automatically a finite extension of $\mathbb{Q}_p$. It is a fact that all such local fields are isomorphic to ones coming from this global construction.

As above, the discrete valuation ring of $\mathcal{O}_{F_\mathfrak{p}} \subset F_\mathfrak{p}$ is the integral closure of $\mathbb{Z}_p$ in $F_\mathfrak{p}$. More generally, if E/F is an extension of number fields and $\mathfrak{P} \subset \mathcal{O}_E$ is a non-zero prime ideal lying over $\mathfrak{p} \subset \mathcal{O}_F$, then $E_\mathfrak{P}$ is naturally a finite extension of $F_\mathfrak{p}$ and $\mathcal{O}_{E_\mathfrak{P}}$ is the integral closure of $\mathcal{O}_{F_\mathfrak{p}}$ in $E_\mathfrak{P}$. It is a standard fact that there is a canonical isomorphism

$$F_\mathfrak{p} \otimes_F E \cong \prod_{\mathfrak{P}|\mathfrak{p}} E_\mathfrak{P}.$$

A similar result holds at the archimedean places. This establishes there is a canonical isomorphism

$$\mathbb{A}_F \otimes_F E \cong \mathbb{A}_E.$$

Hence these is a norm map:

$$N_{E/F} : \mathbb{A}_E \longrightarrow \mathbb{A}_F,$$

induced by the usual norm map. This is a group homomorphism when restricted to the ideles. Recall that a DVR is a Dedekind domain with precisely one non-zero prime ideal. In this case the unique non-zero prime ideal is $\mathfrak{p}\mathcal{O}_{F_\mathfrak{p}}$, and we denote it by $\mathfrak{p}$ again. As above we know that

$$\mathfrak{p}\mathcal{O}_{E_\mathfrak{P}} = \mathfrak{P}^e$$

for $e = e(E_\mathfrak{P}/F_\mathfrak{p})$. It is a straight forward exercise to show that that in this setting $e(\mathfrak{P}/\mathfrak{p}) = e(E_\mathfrak{P}/F_\mathfrak{p})$, so the local and global ramification indexes coinicide. It is a standard fact that If E/F is Galois then $E_\mathfrak{P}/F_\mathfrak{p}$ is Galois.

Proposition. *The Decomposition group at $\mathfrak{P}$, $G(\mathfrak{P}) \subset Gal(E/F)$, is isomorphic to $Gal(E_\mathfrak{P}/F_\mathfrak{p})$.*

Proof. This is proposition 3 of §10 of the chapter on local Fields in Cassel's/Frohlich. □

Number Theory

Alexander Paulin

October 4, 2009

Lecture 8

Profinite Groups

Definition. *Let I be a set together with a reflexive, transitive relation, $\leq$. We say that $(I, \leq)$ is a directed set if given $i_1, i_2 \in I$, there extist $i \in I$ such that $i_1 \leq i$ and $i_2 \leq i$.*

Definition. *Let $(I, \leq)$ be a direct system. An inverse system of topological groups over I is an object $(I, G_i; \phi_i^j)$, where for each $i \in I$, G_i is a topological group and for each $i \leq j$ in I, ϕ_i^j is a morphism: $G_j \longrightarrow G_i$. Moreover, ϕ_i^i is the identity on G_i and if $i \leq j \leq k$, then $\phi_i^j \phi_j^k = \phi_i^k$.*

One should think about an inverse system of topological groups an a particular type of diagram in the category of topological groups.

Let (G_i) be an inverse system of topological groups and form the cartesian product $\prod_{i \in I} G_i$. This is again a topological group giving it the product topology. Let L be the subgroup of all (x_i) in $\prod_{i \in I} G_i$ with the property that whenever $i \leq j$, $\phi_i^j(x_j) = x_i$. We give L the subspace topology. It is clearly closed in $\prod_{i \in I} G_i$. We say that L is the inverse (sometimes projective) limit of (G_i) and we denote it by $L = \varprojlim G_i$. One should view this bject as the limit of the diagram given by the inverse system in the category of topological groups.

We shall view finite groups as topological groups with the discrete topology. A topological group is topologically isomorphic to an inverse limit of finite groups is called a profinite group. If all the finite groups are p- groups are p-groups for some prime p we say it is a pro-p group. By Tychonoff's theorem we deduce that profinite groups are compact. It can also be shown that all profinite groups are totally disconnected. In fact we have the following classification:

Theorem. *A topological group is profinite if and only if it is compact and totally disconnected.*

Proof. This is Theorem 1 of the profinite group chapter of Cassels/Frohlich. □

Essentially the reason is that given $N \subset G$ an open normal subgroup, then by compactness it is of finite index. G is topologically isomorphic to the inverse limit of all quotients G/N. Observe that an open subgroup of a profinite group is automatically closed and of finite index.

Important Special Cases:

1. (H_i) is the family of all normal subgroups of finite index in G. We denote the profinite completion of G by $\varprojlim G/H_i := \hat{G}$. For example $\hat{\mathbb{Z}}$ is the inverse limit over all finite cyclic groups.

2. (H_i) is the family of all normal subgroups of G with index a power of p, for some fixed prime p. Then the pro-p completion of G is $\varprojlim G/H_i : \hat{G}_p$. If G is abelian then $\hat{G} = \prod_p \hat{G}_p$. If $G = \mathbb{Z}$ then $\hat{\mathbb{Z}}_p = \mathbb{Z}_p$ and $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

Profinite Groups in Field Theory

Let F be a field and E/F an algebraic extension. We say that E/F is Galois if fixed field of the F-automorphisms of E is precisely F. In this case we define the Galois group of E/F, denoted $Gal(E/F)$, to be the F- automorphisms of E

Let $(K_i, i \in I)$ be the family of all finite Galois extensions of F contained in E. This set is a direct system, where the relation is given by containment. This induces the structure of an inverse system on $(Gal(K_i/F), i \in I)$, there the morphism are given by restriction.

Proposition. *There is a canonical isomorphism* $Gal(E/F) \cong \varprojlim Gal(K_i/F)$

Proof. This is proposition 1 of the Profinite group chapter of Cassels/Frohlich. □

Hence we may naturally endow $Gal(E/F)$ with the structure of a profinite topological group. By the above $Gal(E/F)$ is compact and totally disconnected. If E/F is finite then this gives the discrete topology on $Gal(E/F)$.

If F is perfect (all finite extensions are separable) then an algebraic closure $\bar{F}$ is Galois over F. We define the absolute Galois group of F to be $G_F := Gal(\bar{F}/F)$. Given another algebraic closure of F the resulting group is canonically isomorphic to $Gal(\bar{F}/F)$, hence the concept is well defined up to canonical isomorphism. If we take the special case $F = \mathbb{F}_p$, then $Gal(\bar{\mathbb{F}}_p/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$.

Fundamental Theorem of Galois Theory. *Let E/F be a Galois extension with Galois group G. Let Σ be the set of all closed subgroups of G and Γ be the set of all fields between E and F. Then $K \longrightarrow Gal(E/K)$ is a bijection from Γ to Σ. An intermediate field K is Galois over F if and only if the corresponding closed subgroup is normal. Here $Gal(K/F) \cong G/Gal(E/K)$. The intermediate fields which are finite over F correspond to the open subgoups (which are automatically open).*

Proof. This is Theorem 2 of the profinite groups chapter of Cassels/Frohlich. □

Hence if F is perfect the absolute Galois group has all possible Galois groups of finite extensions of F as quotients. Intuitively we should think about $Gal(\bar{F}/F)$ as a way of *binding* together all finite Galois groups for F. This will unify many of the constructions we have already encountered.

Let E/F be an extension of perfect fields. Let us fix algebraic closures $\bar{E}$ and $\bar{F}$. By construction, there must exist an F-embedding $\phi : \bar{F} \longrightarrow \bar{E}$. Because $\bar{F}/F$ is Galois we know if φ is another such embedding then $\varphi = \phi\sigma$ for some $\sigma \in Gal(\bar{F}/F)$. The embedding ϕ induces a continuous embedding $Gal(\bar{E}/E) \longrightarrow Gal(\bar{F}/F)$. The embedding induced by φ differs from that induced by ϕ by conjugation by σ. Hence the absolute Galois group of E embeds in the absolute Galois group of F, but only up to conjugation.

Absolute Galois groups of Number Fields

Let F be a number field. F is of characteristic zero hence is perfect. Let us denote the absolute Galois group by G_F. By the above considerations we know that G_F holds the information of all finite Galois extensions of F. By the above we know that G_F embeds in $G_{\mathbb{Q}}$ (up to conjugation) as an open normal subgroup. It is no exaggeration to say that most of algebraic number theory is just the study of $G_{\mathbb{Q}}$. This topological group is in some senses *the* arithmetic group. Conjecturally it has all finite groups as quotients! Really we want to understand as much about this group as we can. As we shall see it's internal complexity is *mind blowing*. The rest of the course will be exclusively devoted to this group. First let's try and relate it back to ideas we've already covered.

Let $\mathfrak{p} \subset \mathcal{O}_F$ be a non-zero prime ideal. We have a canonical embedding $F \subset F_{\mathfrak{p}}$. Fix an embedding $\phi : G_{F_{\mathfrak{p}}} \longrightarrow G_F$ (equivalently an embedding $\bar{F} \to \bar{F}_{\mathfrak{p}}$) . Let E/F be a finite extension contained in $\bar{F}$. It corresponds by the fundamental theorem to an open subgroup $G_E \subset G_F$. Taking the preimage of this subgroup under ϕ we get an open subgroup $H \subset G_{F_{\mathfrak{p}}}$. This subgroup corresponds to some finite Galois extension $K/F_{\mathfrak{p}}$. It is not hard to see that $K = F_{\mathfrak{p}}E$, via the embedding ϕ. Note that this field is a finite extension is of $F_{\mathfrak{p}}$, which is complete. Hence it's absolute value is uniquely determined. We also know that up to equivalence the only absolute values on E extending the one on F induced by $\mathfrak{p} \subset \mathcal{O}_F$ come from non-zero primes $\mathfrak{P} \subset \mathcal{O}_E$ diving $\mathfrak{p}$. We deduce that that there exists a unique non-zero prime ideal $\mathfrak{P} \subset \mathcal{O}_E$ such that K is topologically isomorphic to $E_{\mathfrak{P}}$. Moreover $Gal(K/F_{\mathfrak{p}})$ is equal to the decomposition group at $\mathfrak{P}$. Recall that embeddings of $G_{F_{\mathfrak{p}}}$ in G_F differ only by conjugation. If φ equals $\phi\sigma$ for $\sigma \in G_F$ then if we carry out the above procedure for φ, K will be topologically isomorphic to $E_{\sigma\mathfrak{P}}$.

Definition. *Let E/F and K/F be two finite extensions contained in the finite extension L/F. We say that the non-zero prime ideals $\mathfrak{P} \subset \mathcal{O}_E$, $\mathsf{P} \subset \mathcal{O}_K$ and $\mathcal{P} \subset \mathcal{O}_L$ over $\mathfrak{p}$ is compatible if $\mathcal{P}|\mathfrak{P}$ and $\mathcal{P}|\mathsf{P}$.*

If E/F is an algebraic extension then by a compatible system of non-zero primes lying over $\mathfrak{p}$ we mean a choice of non-zero prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ for every K/F finite such that they

are compatible in the above sense. Observe that to stipulate a compatible system we only need to make a choice for all finite Galois extensions. To conclude, **to give a compatible system of non-zero primes ideal lying over $\mathfrak{p}$ in the extension $\bar{F}/F$ is the same as giving an embedding $\bar{F} \to \bar{F}_{\mathfrak{p}}$ and G_F acts transitively on this set.**

Maximal Unramified Extensions

Let E/F be an extension of fields with $E \subset \bar{F}$. We say that E is unramified at $\mathfrak{p}$ if all finite extensions of F contained in E are unramified at $\mathfrak{p}$. Let E, K be two finite Galois extensions of F contained in $\bar{F}$. We know by the properties of Frobenius elements that

$$E, K \text{ unramified at } \mathfrak{p} \Rightarrow EK \text{ unramified at } \mathfrak{p}.$$

This result is also true when we omit the finiteness condition. Hence given any set of place S containing all archimedean places, there is a maximal extension of F contained in $\bar{F}$ which is unramified at all non-zero primes not contained in S. We denote this extension by F_S. It is a Galois extension of F and we denote the Galois group by $G_{F,S}$. It is naturally a quotient of G_F by the fundamental theorem and by construction

$$G_{F,S} = \varprojlim_{E/F \ \mathit{Finite} \ \mathit{Galois} \ \mathit{Unramified}} Gal(E/F).$$

Let us fix a compatible system of non-zero primes lying over $\mathfrak{p} \notin S$, which we denote by ϕ. By the compatibility of Frobenius elements under extensions and compositions we know that for such $\mathfrak{p}$ there is a canonical frobenius element $Frob_{\mathfrak{p},\phi} \in G_{F,S}$. This is just just the usual choice of Frobenius for each Galois extension.

As in the finite case, two different choices of compatible system over $\mathfrak{p} \notin S$ will give conjugate Frobenius elements. By transitivity of $G_{F,S}$ on the set of compatible systems over $\mathfrak{p}$ we get a well defined conjugacy class $Frob_{\mathfrak{p}} \subset G_{F,S}$. Let us assume that S is finite. Let Σ be a collection of representatives for each class $Frob_{\mathfrak{p}} \subset G_{F,S}$ for $\mathfrak{p} \notin S$. The Tchebotarev density theorem implies that Σ is dense in $G_{F,S}$, after giving it the profinite topology. This is very important.

Recall that an embedding $\phi : \bar{F} \to \bar{F}_{\mathfrak{p}}$ is the same thing as choosing a compatible system of non-zero prime ideals over $\mathfrak{p}$ in the extension $\bar{F}/F$. Again this is the same as fixing an embedding $\phi : G_{F_{\mathfrak{p}}} \to G_F$. Next time we shall see how to determine $Frob_{\mathfrak{p},\phi}$ directly from this embedding.

Number Theory

Alexander Paulin

October 6, 2009

Lecture 9

Maximal Unramified Extensions

Let F be a number field and $\bar{F}$ a fixed algebraic closure. Let $\mathfrak{p} \subset \mathcal{O}_F$ be a non-zero prime ideal. Let E/F be an extension of fields with $E \subset \bar{F}$. Note that E is non necessarily finite over F. We say that E is unramified at $\mathfrak{p}$ if all finite extensions of F contained in E are unramified at $\mathfrak{p}$. Let E, K be two finite extensions of F contained in $\bar{F}$. It is true that:

$$E, K \text{ unramified at } \mathfrak{p} \Rightarrow EK \text{ unramified at } \mathfrak{p}.$$

We deduce that given any set of places S containing all archimedean places, then F_S, the union of all finite extensions of F unramified outside S is a field. F_S is the maximal extension of F contained in $\bar{F}$ which is unramified at all non-zero prime ideals not contained in S. It is a Galois extension of F and we denote the Galois group by $G_{F,S}$. By the fundamental theorem of Galois theory it is naturally a quotient of G_F. If I is the direct system of finite, unramified away from S, Galois extensions of F contained in $\bar{F}$ then by construction

$$G_{F,S} = \varprojlim_{E \in I} Gal(E/F).$$

Let us fix a compatible system of non-zero primes lying over $\mathfrak{p} \notin S$, which we denote by ϕ (equivalently an embedding $\phi : \bar{F} \to \bar{F}_{\mathfrak{p}}$). By the compatibility of Frobenius elements under extensions and compositums we know that for such $\mathfrak{p}$ there is a canonical frobenius element $Frob_{\mathfrak{p},\phi} \in G_{F,S}$. In terms of the inverse limit if we have

$$Frob_{\mathfrak{p},\phi} = \varprojlim_{E \in I,\, \mathfrak{P} \subset \mathcal{O}_E,\, \mathfrak{P} \in \phi} (E/F, \mathfrak{P}).$$

As in the finite case, two different choices of compatible system over $\mathfrak{p} \notin S$ will give conjugate Frobenius elements. By transitivity of $G_{F,S}$ on the set of compatible systems over $\mathfrak{p}$ we get a well defined conjugacy class $Frob_{\mathfrak{p}} \subset G_{F,S}$. Let us assume that S is finite. Let Σ be a collection of representatives for each class $Frob_{\mathfrak{p}} \subset G_{F,S}$ for $\mathfrak{p} \notin S$. The Tchebotarev density theorem implies that Σ is dense in $G_{F,S}$, after giving it the profinite topology. This

is very important.

Recall that an embedding $\phi : \bar{F} \to \bar{F}_{\mathfrak{p}}$ is the same thing as choosing a compatible system of non-zero prime ideals over $\mathfrak{p}$ in the extension $\bar{F}/F$. Again this is the same as fixing an embedding $\phi : G_{F_{\mathfrak{p}}} \to G_F$. So for every $\mathfrak{p} \subset \mathcal{O}_F$ a non-zero prime ideal we get a canonical (up to conjugation) subgroup of G_F. To try to understand G_F better we will first attempt to understand these subgroups. As we shall see, this task is already formidable.

Absolute Galois Groups of Local Fields

Let F be a non-archimedean local field of characteristic zero and residue characteristic p. Recall that this is equivalent to F being a finite extension of $\mathbb{Q}_p$. Fix an algebraic closure $\bar{F}$. We want to study G_F. Our first attack will be to decompose G_F into certain subgroups whose quotients are easy to understand.

Observe that as in the global case the compositum of two unramified extensions of F contained in $\bar{F}$ is again unramified. This also makes sense for infinite extensions.

Definition. *The maximal unramified extension of F contained in $\bar{F}$, denoted F^{nr}, is the union of all finite unramifed extensions of F contained in $\bar{F}$.*

By the previous remark we see this definition makes sense. In fact F^{nr} is the union of the fields of m^{th} roots of unity in $\bar{F}$ for m coprime to p. For a proof of this fact see the bottom of page 28 of Cassels/Fohlich. It should be noted that even though F^{nr} naturally comes with a unique absolute value extending that on F it is not complete. The residue field of F^{nr} equals $\bar{\mathbb{F}}_F$, for a fixed algebraic closure. If π is a uniformiser for F then π is also a uniformiser for F^{nr}. F^{nr}/F is Galois and by construction

$$Gal(F^{nr}/F) \cong \varprojlim_{\bar{F}/E/F \text{ finite Galois unramified}} Gal(E/F).$$

But recall that E/F finite, unramified and Galois then $Gal(E/F) \cong Gal(\mathbb{F}_E/\mathbb{F}_F)$. This latter group is isomorphic to the the cyclic group of order $[E : F]$. It is true that given any $n \in \mathbb{N}$ there exists a unique unramified extension of F of degree n contained in $\bar{F}$. One can actually give a direct construction of such an extension using something called Witt vectors - see the first section of Serre's book on Local Fields. Even though F^{nr} is not complete we may still talk about tamely, wildly and totally ramified extensions of it because its residue field is perfect. In particular, every finite extension of F^{nr} , contained in $\bar{F}$ is totally ramified. We deduce that there is a canonical topological isomorphism

$$Gal(F^{nr}/F) \cong G_{\mathbb{F}_F} \cong \hat{\mathbb{Z}}.$$

The canonical Frobenius element in $G_{\mathbb{F}_F}$ corresponds to $1 \in \mathbb{Z} \subset \hat{\mathbb{Z}}$.

Recall that $Gal(F^{nr}/F)$ is isomorphic to the quotent of G_F by the subgroup $Gal(\bar{F}/F^{nr})$. Hence there is a short exact sequence

$$0 \longrightarrow Gal(\bar{F}/F^{nr}) \longrightarrow G_F \longrightarrow \hat{\mathbb{Z}} \longrightarrow 0.$$

In particular there is a natural homomorphism $\varphi : G_F \to \hat{\mathbb{Z}}$.

Definition. *The Weil group of F , denoted W_F, is the pre-image of $\mathbb{Z}$ under φ. The inertia subgroup of F, denoted I_F, is the kernel of φ.*

Observe that because $\mathbb{Z} \subset \hat{\mathbb{Z}}$ is dense, $W_F \subset G_F$ is dense. We have the exact sequence:

$$0 \longrightarrow I_K \longrightarrow W_F \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Note that $I_K = Gal(\bar{F}/F^{nr})$. The inertia subgroup is naturally the inverse limit of all finite inertia groups of finite Galois extensions of F contained in $\bar{F}$. Observe that W_K is the disjoint union of right cosets of I_K indexed by $\mathbb{Z}$. We topologize W_F by giving I_K the subspace topology induced from $I_K \subset G_F$ and then endowing W_F with the disjoint union topology. This makes W_F a topological group. **Warning**: This is not the subspace topology induced by $W_F \subset G_F$, however the inclusion is still continuous. It is hard to justify why we do this, but it will become clear when we introduce the local Langlands correspondence. If E/F is a finite extension then W_E is naturally an open subgroup of W_F, and is hence of finite index . If E/F is Galois then W_E is normal in W_F and the quotient is isomorphic to $Gal(E/F)$.

Tamely Ramified Extensions

Let F be a no-archimedean local ring of characteristic zero and residue characteristic p. Recall that a finite extension E/F contained in $\bar{F}$ is tamely ramified if p does not divide $e(E/F)$. This still makes sense even if we drop the completeness hypothesis. We can also relax the condition that the residue field is finite. It merely needs to be perfect.

Proposition. *Let E/F and K/F be two finite extensions contained in $\bar{F}$.*

$$E/F \text{ and } K/F \text{ are tamely ramified } \iff EK/F \text{ is tamely ramified.}$$

Proof. This is Corollary 2 of §8 of the Local Fields chapter of Cassels/Frohlich. □

Definition. *We define the maximal tamely ramified extension, $F^{tr} \subset \bar{F}$ to be the union of all tamely ramified extensions of F in $\bar{F}$.*

Note that by the proposition this makes sense. Again F^{tr}/F is a Galois extension and $F^{nr} \subset F^{tr}$. If E/F^{nr} is a finite extension contained in $\bar{F}$ then it is tamely ramified if and only if it is contained on F^{tr}. Also observe that such an extension must be totally ramified.

Proposition. *Let E/F^{nr} be a finite tamely ramified Galois extension contained in $\bar{F}$ (and hence in F^{tr}), of degree e. Then $\exists \pi \in F^{nr}$ a uniformiser (i.e a generator of the maximal ideal of the valuation ring of F^{nr}) such that $E = F^{nr}(\pi^{1/e})$.*

Proof. This is proposition 1 of §8 of the Local Fields chapter of Cassels/Frohlich. □

Number Theory

Alexander Paulin

October 12, 2009

Lecture 10

Let F be a non-archimedean local field of characteristic zero and residue characteristic p. Recall that this is equivalent to F being a finite extension of $\mathbb{Q}_p$. Fix an algebraic closure $\bar{F}$. Recall that we defined $F^{nr} \subset \bar{F}$, the maximal unramified extension of F, as the union of all finite unramified extensions of F in $\bar{F}$. Similarly we defined $F^{tr} \subset \bar{F}$, the maximal tamely ramified extension of F, as the union of all finite tamely extensions of F in $\bar{F}$. There was a natural inclusion $F^{nr} \subset F^{tr}$. At the end of the last lecture we saw that it we fix a uniformiser $\pi \in F$, then F^{tr} is the union of all fields $F^{nr}(\pi^{1/e})$, for all $e \in \mathbb{N}$ coprime to p. These are all Galois extensions. We should note that this $\pi^{1/e}$ is only well defined up to a multiple of a primitive e^{th} root of unity, contained in F^{nr}. It is in fact true that $F^{nr}(\pi^{1/e})$ is the unique tame extension of F^{nr} contained in $\bar{F}$ of degree e. Because of the fact that F^{nr} contains a primitive e^{th} root of unity for all e coprime to p $F^{nr}(\pi^{1/e})/F^{nr}$ is an example of a Kummer extension. Kummer theory is the study of Galois extensions where the base field contains many primitive roots of unity. Let $\mu_e \subset F^{nr*}$ be the subgroup of e^{th} roots of unity.

Lemma. *The homomorphism*

$$\begin{aligned} Gal(F^{nr}(\pi^{1/e})/F^{nr}) &\longrightarrow \mu_e \\ \sigma &\longrightarrow \frac{\sigma(\pi^{1/e})}{\pi^{1/e}} \end{aligned}$$

is an isomorphism.

Proof. This is a fundamental result in basic Kummer theory. It is a special case of lemma 1 (page 90) of the Cyclotomic Fields chapter of Cassels/Frohlich. □

Combining all of the above we see that there is a natural topological isomorphism:

$$Gal(F^{tr}/F^{nr}) \cong \varprojlim_{e \in \mathbb{N},\ (e,p)=1} Gal(F^{nr}(\pi^{1/e})/F^{nr}) \cong \varprojlim_{e \in \mathbb{N},\ (e,p)=1} \mu_e.$$

If $e, f \in \mathbb{N}$ such that $e|f$ then the transition map $\mu_f \to \mu_e$ is $\zeta \to \zeta^{f/e}$. If we fix a compatible collection of e^{th} roots of unity in F^{nr} for all $e \in \mathbb{N}$ coprime to p, then this establishes a (non-canonical) topological isomorphism:

$$Gal(F^{tr}/F^{nr}) \cong \varprojlim_{e\in\mathbb{N},\,(e,p)=1} \mu_e \cong \varprojlim_{e\in\mathbb{N},\,(e,p)=1} \mathbb{Z}/e\mathbb{Z} \cong \prod_{q\neq p} \mathbb{Z}_q.$$

Hence there is a short exact sequence:

$$0 \longrightarrow \prod_{q\neq p} \mathbb{Z}_q \longrightarrow Gal(F^{tr}/F) \longrightarrow \hat{\mathbb{Z}} \longrightarrow 0.$$

This sequence is not trivial because there are finite tamely ramified extensions of F which are not abelian, thus $Gal(F^{tr}/F)$ is not abelian. Note that if $\sigma \in \hat{\mathbb{Z}}$ and $\tilde{\sigma} \in Gal(F^{tr}/F)$ is any lift then for $\tau \in \prod_{q\neq p} \mathbb{Z}_q$, $\sigma(\tau) = \tilde{\sigma}\tau\tilde{\sigma}^{-1}$ is independent of the lift. This is because $\prod_{q\neq p} \mathbb{Z}_q$ is Abelian. hence there is a natural action of $\hat{\mathbb{Z}}$ on $\prod_{q\neq p} \mathbb{Z}_q$. Note that the frobenius element in $\hat{\mathbb{Z}}$ ($1 \in \hat{\mathbb{Z}}$) generates $\mathbb{Z} \subset \hat{\mathbb{Z}}$, which is dense. Because the action is contiuous if we know how frobenius acts then we know the whole action.

Theorem. *Frobenius acts on $\prod_{q\neq p} \mathbb{Z}_q$ via multiplication by $|\mathbb{F}_F|$.*

Proof. We'll outline the basic argument: It is enough to treat the case of E/F^{nr} a finite tamely ramified Galois extension of degree e. Then we know that $Gal(E/F^{nr})$ is isomorphic to μ_e. Hence it is sufficient to prove that frobenius acts on $Gal(E/F^{nr}) \cong \mu_e$ by $\zeta \to \zeta^{|\mathbb{F}_F|}$. To prove this observe that

1. $Gal(E/F^{nr}) \cong \mu_e$ preserves the action of $Gal(F^{nr}/F)(\mu_e \subset F^{nr})$.
2. If ζ is a primitive root of unity of order prime to p then Frobenius sends ζ to $\zeta^{|\mathbb{F}_F|}$.

□

If E/F^{tr} is a finite extension contained in $\bar{F}$ then by theorem 1 on page 29 of Cassels/Frohlich, we know that E/F^{nr} is wildly ramified and in face $[E : F^{tr}]$ is a power of p. In particular this tells us that $Gal(\bar{F}/F^{tr})$ is a pro-p group. This group is quite mysterious - we can't really decompose it in the same was as $Gal(F^{tr}/F)$.

In summary: **Let F be a finite extension of $\mathbb{Q}_p$. Let $\bar{F}$ be fixed algebraic closure. We have a tower of Galois field extensions $F \subset F^{nr} \subset F^{tr} \subset \bar{F}$. $Gal(\bar{F}/F^{tr})$ is a pro-p subgroup of G_F, whose quotient is naturally isomorphic to $Gal(F^{tr}/F)$. The subgroup $Gal(F^{tr}/F^{nr}) \subset Gal(F^{tr}/F)$ is non-canonically topologically isomorphic to $\prod_{q\neq p} \mathbb{Z}_q$. The quotient is naturally isomorphic to $Gal(F^{nr}/F)$, which is in turn naturally topologically isomorphic to $\hat{\mathbb{Z}}$.**

That's about as far as this decomposition approach will work - there is no easy description of the pro-p part of G_F. Instead let's try another attack.

Local Class Field Theory

Again let F be a non-archimedean local field of characteristic zero and residue characteristic p. Let $\bar{F}$ be a fixed algebraic closure. We say that E/F, a finite Galois extension contained in $\bar{F}$, is Abelian if $Gal(E/F)$ is Abelian. Taking the compositum of two Abelian extension within $\bar{F}$ is again an Abelian extension.

Definition. *The maximal Abelian extension of F, denoted F^{ab} is the union of all finite abelian extensions of F contained in $\bar{F}$.*

By the previous remark F^{ab} is a field. Observe that unramified Galois extensions of F are Abelian (they are cyclic), hence $F^{nr} \subset F^{ab}$. As before F^{ab}/F is Galois. The aim of local class field theory is to give an independent description of $Gal(F^{ab}/F)$. By the fundamental theorem of Galois theory this is basically the same as classifying all finite Abelian extensions of F.

If G is a topological group and $M \subset G$ is it's commutator subgroup, then we define G^{ab}, the topological abelianisation of G to be $G/\bar{M}$, there $\bar{M}$ is the closure of M in G. It is an easy exercise to that $Gal(F^{ab}/F) \cong G_F^{ab} :=$. If W_F is the Weil group then there is a natural inclusion $W_F^{ab} \subset G_F^{ab}$ is dense. There are two natural short exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_F^{ab} & \xrightarrow{\theta_F} & G_F^{ab} & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle identity} & & \uparrow{\scriptstyle inclusion} & & \uparrow{\scriptstyle inclusion} & & \\ 0 & \longrightarrow & I_F^{ab} & \longrightarrow & W_F^{ab} & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

where I_F^{ab} is isomorphic to $Gal(F^{ab}/F^{ur})$. Let us fix a lift of frobenius $frob \in W_F^{ab}$. Also recall that if G is a topological group and $H \subset G$ is an open subgroup then there is a transfer map on topological abelianisations: $G^{ab} \to H^{ab}$. For a detailed description of this map see Tate's "Number Theortic Background" in the Corvallis conference proceedings on Automorphic Representations.

Fundamental Theorem of Local Class Field Theory. *Let F be a finite extension of $\mathbb{Q}_p$ and $\bar{F}$ a fixed algebraic closure. Let E/F be finite Abelian Galois extension contained in $\bar{F}$. Let $N_{E/F} : E^* \to F^*$, denote the norm map.*

1. *There is a local reciprocity isomorphism:*

$$\theta_{E/F} : F^*/N_{E/F}(E^*) \to Gal(E/F).$$

2. *let $\tilde{F} := \varprojlim F^*/N_{E/F}(E^*)$, where the limit is taken over all finite Abelian Galois extension contained in $\bar{F}$. Then the local reciprocity isomorphisms induce a topological isomorphism $\tilde{F} \cong G_F^{ab}$. The natural injective map*

$$\theta : F^* \to \tilde{F} \cong G_F^{ab}$$

is continuous and maps isomorphically only W_F^{ab}.

3. *$\theta_F(\mathcal{O}_F^*) = I_F^{ab}$ and if $\pi_F \in F^*$ is a uniformiser then $\theta(\pi_F) \in frob\ I_F^{ab}$. (One should note that there is another convention which gives $\theta_F(\pi_F) \in frob^{-1} I_F^{ab}$)*

4. *For E/F a finite extension we have the following commutative diagrams:*

$$\begin{array}{ccc} E^* & \xrightarrow{\theta_E} & W_E^{ab} \\ \downarrow{\scriptstyle N_{E/F}} & & \downarrow{\scriptstyle inclusion} \\ F^* & \xrightarrow{\theta_F} & W_F^{ab} \end{array}$$

$$\begin{array}{ccc} F^* & \xrightarrow{\theta_F} & W_F^{ab} \\ \downarrow{\scriptstyle inclusion} & & \downarrow{\scriptstyle transfer} \\ E^* & \xrightarrow{\theta_E} & W_E^{ab} \end{array}$$

Proof. Unsurprisingly this is a deep pretty deep theorem and is not easy to prove. See Serre's Chapter of Cassels/Frohlich. Interestingly the proof there is entirely local, with no appeal to number fields. Historically the local case was first deduced from the global version of class field theory, which we'll encounter soon. Conversely, the modern generalisation of class field theory are much better understood in the local case than in the global. □

Number Theory

Alexander Paulin

October 13, 2009

Lecture 11

Let F be a non-archimedean local field of characteristic zero and residue characteristic p. Recall that this is equivalent to F being a finite extension of $\mathbb{Q}_p$. Fix an algebraic closure $\bar{F}$. Recall that if F^{ab} is the maximal abelian extension of F contained in $\bar{F}$ then the main theorem of local class field theory asserts that there is a natural topological isomorphism

$$W_F^{ab} \cong GL_1(F).$$

There are two possible normalisations depending on whether we choose to send a uniformiser $\pi \in F^*$ to an element of the coset (of I_F^{ab}) containing a lift of frobenius or it's inverse.

Let K be a topological field. Let $\chi : G_F \longrightarrow GL_1(K)$ be a continuous (for the profinite topology on G_F) character. Observe that by continuity we know that χ must factor through the quotient

$$\chi : G_F \longrightarrow G_F^{ab} \longrightarrow GL_1(K).$$

Recall that $W_F^{ab} \subset G_F^{ab}$ is dense, hence χ is completely determined by it's restriction to W_F^{ab}. We deduce that as a consequence of local class field theory there is a canonical (up to a choice of normalisation) bijection between the two sets

$$\{\text{Continuous one dimensional } K\text{-vector space representations of } W_F \ \}$$

$$\updownarrow$$

$$\{\text{Continuous one dimensional } K\text{-vector space representations of } GL_1(F) \ \}$$

This seemingly innocuous observation will be the key to the higher dimensional generalisation of local class field theory. What I mean by this is that it is natural to consider the set

$$\{\text{Isomorphism classes of continuous } n\text{-dimensional } K\text{-vector space representations of } W_F, \text{ for some } n \in \mathbb{N} \ \}$$

To what should this set correspond? It is not at all obvious. We shall address this issue when we consider the local Langlands correspondence.

To conclude this section we should observe that if we choose $K = \mathbb{C}$ then a continuous representation of W_F (or G_F) on a finite dimensional complex vector space is automatically continuous for the discrete topology on $\mathbb{C}$. This is because the topology of $\mathbb{C}$ is extremely incompatible with the totally disconnected topology on W_F. Recall that W_F is not compact, where as G_F is. Hence any continuous representation

$$\rho : G_F \longrightarrow GL_n(\mathbb{C}),$$

has open kernel, and hence has finite image. Conversely a continuous representation

$$\rho' : W_F \longrightarrow GL_n(\mathbb{C}),$$

extends to a representation of G_F if and only if its image is finite. In this case we say that ρ' is of Galois-type. Not all such ρ' are of Galois-type. In the one dimensional case a character is of Galois type if and only if the image of a frobenius lift is a root of unity. An elegant survey of these results can be found in §2 of Tate's "Number Theoretic Background" article.

Global Class Field Theory

Let $F/\mathbb{Q}$ be a number field. A number field is an example of a *global* field, a concept we will not make precise. Let $\bar{F}$ be a fixed algebraic closure of F. As in the local case, if E/F is a finite Abelian Galois extension contained in $\bar{F}$ we say that E/F is Abelian. The compositum of two finite Abelian extensions extensions (in $\bar{F}$) is again Abelian.

Definition. *The maximal Abelian extension of F, denoted F^{ab} is the union of all finite abelian extensions of F contained in $\bar{F}$.*

By the previous remark F^{ab} is a field. F^{ab}/F is Galois and we have

$$G_F^{ab} \cong Gal(F^{ab}/F) \cong \varprojlim_{\bar{F}/E/F \ finite \ Ablian} Gal(E/F).$$

The aim of Global Class Field theory is to give an explicit description of this group. For $F = \mathbb{Q}$ this is essentially achieved by the following famous theorem of Kronecker and Webber:

Theorem. *Let $E/\mathbb{Q}$ be a finite belian extension contained in a fixed algebraic closure $\bar{\mathbb{Q}}$. Then $\exists n \in \mathbb{N}$ such that $E \subset \mathbb{Q}(\zeta_n)$, where $\zeta_n \in \bar{\mathbb{Q}}$ is a primitive n^{th} root of unity.*

Recall that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Abelian with a canonical isomorphism:

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Hence we deduce, via the Kronecker-Webber theorem that there is a canonical topological isomorphism:

$$G_{\mathbb{Q}}^{ab} \cong Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \varprojlim_{n\bar{\in}\mathbb{N}} Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \varprojlim_{n\bar{\in}\mathbb{N}} (\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{p \ prime} \mathbb{Z}_p^*.$$

Class Field Theory seeks to generalise this type of result to all number fields. The generalisation is much more difficult to prove, and its completion was the high point of early twentieth century number theory.

Let E/F be a finite Abelian extension (in $\bar{F}$). Let S be the set of all archimedean places of F together with the non-zero primes ideals $\mathfrak{p} \subset \mathcal{O}_F$ which are ramified in E/F. In particular S is finite. Let $\mathfrak{I}_F^S$ denote the free abelain subgroup of the fractional ideal group of F, generated by the non-zero prime ideals not contained in S. In particular $\mathfrak{p}$ is unramified in E/F if and only if $\mathfrak{p} \notin S$. Because E/F is Abelian, given $\mathfrak{p} \notin S$ there is a well defined Frobenius element $frob_{\mathfrak{p}} \in Gal(E/F)$. This allows us to define the group homomorphism:

$$\begin{array}{rcl} F_{E/F} : \mathfrak{I}_F^S & \longrightarrow & Gal(E/F) \\ \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{n_{\mathfrak{p}}} & \longrightarrow & \prod_{\mathfrak{p} \notin S} frob_{\mathfrak{p}}^{n_{\mathfrak{p}}} \end{array}$$

This makes sense only because E/F is Abelian. Without this assumption this is not possible.

Let $J_F = GL_1(\mathbb{A}_F)$, the ideles of F. Similarly let J_E denote the ideles of E. Recall that there is a canonical embedding $F^* \subset J_F$. Let $J_K^S \subset J_K$ denote the subgroup whose entries for $v \in S$ have value 1. Recall that if $x \in J_K$ then it has a non-unit component at only a finite number of places. Hence there is a group homomorphism:

$$\begin{array}{rcl} (.)^S : J_K^S & \longrightarrow & \mathfrak{I}_F^S \\ x & \longrightarrow & (x)^S := \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})} \end{array}$$

Let $C_F := J_K/F^*$ and $C_E : J_E/E^*$, be the respective idele class groups. The norm homomorphism $N_{E/F} : J_E \longrightarrow J_F$ naturally descends to a homomorphism: $N_{E/F} : C_E \longrightarrow C_F$. We will freely switch between these viewpoints.

Fundamental Theorem of Global Class Field Theory. *Let F be a number field and $\bar{F}$ a fixed algebraic closure. Let E/F be a finite abelian extension contained in $\bar{F}$.*

1. *There exists a unique, continuous, surjective group homomorphism (the Artin reciprocity homomorphism)*
$$\psi_{E/F} : J_K \longrightarrow Gal(E/F),$$
such that (i) $\psi_{E/F}(F^*) = 1$ and (ii) $\psi_{E/F}(x) = F_{E/F}((x)^S)$ for all $x \in J_K^S$. Hence ψ is a continuous homomorphism from C_F onto $Gal(E/F)$.

2. *The kernel of $\psi_{E/F}$ is $F^* N_{E/F}(J_E)$ and hence induces an isomorphism of $C_F/N_{E/F}(C_E)$ on to $Gal(E/F)$.*

3. *If $F \subset E \subset M$ are finite abelian extensions, then the diagram:*

$$\begin{array}{ccc} C_F/N_{M/F}(C_M) & \xrightarrow{\psi_{M/F}} & Gal(M/F) \\ \Big\downarrow j & & \Big\downarrow restriction \\ C_F/N_{E/F}(C_E) & \xrightarrow{\psi_{E/F}} & Gal(E/F) \end{array}$$

commutes. (j is the natural surjective map which exists because $N_{M/F}(C_M) \subset N_{E/F}(C_E)$.)

4. *(Existence Theorem) For every open subgroup N of finite index in C_F, there exists a unique finite Abelian extension E/F (in $\bar{F}$) such that $N_{E/F}(C_E) = N$.*

Proof. This is a deep theorem (deeper than the local field case). It is proven in Tate's article on Global Class Field Theory in Cassels/Frohlich. The original proof was very messy and technical. The proof given by Tate is much slicker using Group cohomology. To give a complete survey of it would take an entire course. Somehow though knowing the proof is unenlightening - it hints at none of the higher dimensional generalisations. Understanding the statement is the main thing. □

Number Theory

Alexander Paulin

November 28, 2009

Lecture 12

Let $F/\mathbb{Q}$ be a number field. Let $\bar{F}$ be a fixed algebraic closure of F. Let F^{ab} be the maximal abelian extension. Let J_F denote the ideles and $C_F = J_F/F^*$ denote the idele class group. For E/F a finite Abelian extension (contained in $\bar{F}$) let $N_{E/F} : C_E \longrightarrow C_F$ denote the natural norm homomorphism. We say last time that there is a natural isomorphism (Artin reciprocity map) $\psi_{E/F} : C_F/N_{E/F}(C_E) \cong Gal(E/F)$. These maps are all compatible under restriction hence we get a topological isomorphism:

$$\psi : \varprojlim_{\bar{F}/E/F \ finite \ abelian} C_F/N_{E/F}(C_E) \cong Gal(F^{ab}/F).$$

The existence theorem (part (iv) of the main theorem) tells us that ψ can further be interpreted as

$$\psi : \varprojlim_{N \subset C_F \ open, \ finite \ index} C_F/N \cong Gal(F^{ab}/F).$$

Thus we obtain the natural reciprocity homomophism :

$$\psi_F : C_F \longrightarrow Gal(F^{ab}/F).$$

It is a fact ψ_F is surjective and the kernel is precisely the connected component of C_F containing the identity, denoted by D_F. For G a topological group we denote by G^o, the connected component containing the identity. Then $(\prod_{v|\infty} F_v^*)^o$ is contained in the kernel of $\psi_F : J_F \longrightarrow G_F^{ab}$. In fact the kernel is precisely the closure of $F^*(\prod_{v|\infty} F_v^*)^o \subset J_F$. In the case $F = \mathbb{Q}$, $C_{\mathbb{Q}}$ is topologically isomorphic to

$$\mathbb{R}_{>0} \times \prod_{p \ prime} \mathbb{Z}_p^*.$$

Hence the connected component containing the identity is just

$$D_{\mathbb{Q}} = \mathbb{R}_{>0} \times \prod_{p \ prime} \{1\}.$$

and we recover the chief consequence of the Kronecker-Webber theorem:

$$G_{\mathbb{Q}}^{ab} \cong \prod_{p\ prime} \mathbb{Z}_p^*.$$

Similarly if $F/\mathbb{Q}$ is a quadratic extension (degree 2) such that it has only one archimedean place (a complex conjugate pair) then the connected component of C_F containing the identity can be given an explicit description. This is the subject of complex multiplication. It turns out that in this case the there is a link between G_F^{ab} and an elliptic curve with some special properties. Note that in both cases there is only one archimedean place. In general if there is more than one archimedean place no such explicit description of the connected component of C_F containing the identity is known. This is the principle reason that proving Class Field Theory is so hard in general.

There is a global equivalent of the Weil group of F, denoted W_F (See Tate's "Number Theoretic Background" article). There is no known explicit description of W_F. What is true is that $W_F^{ab} \cong C_F$ canonically. Unlike in the local case there is a natural surjective homomorphism $W_F \longrightarrow G_F$. This induces a surjective homomorphism $C_F \cong W_F^{ab} \longrightarrow G_F^{ab}$, which turns out to be the Reciprocity map ψ_F.

We will finish this section by considering how these isomorphism behave under finite extension. Let E/F be a finite extension (contained in $\bar{F}$). Hence we have the natural open (thus closed) inclusion $G_E \subset G_F$. This induces the inclusion $G_E^{ab} \subset G_F^{ab}$. As in the local case we have a transfer homomorphism $G_F^{ab} \longrightarrow G_E^{ab}$. The Global Artin reciprocity maps behave well under inclusion and transfer, i.e. we have the following commutative diagrams:

$$\begin{array}{ccc} J_E^* & \xrightarrow{\psi_E} & G_E^{ab} \\ \downarrow{\scriptstyle N_{E/F}} & & \downarrow{\scriptstyle inclusion} \\ J_F & \xrightarrow{\psi_F} & G_F^{ab} \end{array}$$

$$\begin{array}{ccc} J_F^* & \xrightarrow{\psi_F} & G_F^{ab} \\ \downarrow{\scriptstyle inclusion} & & \downarrow{\scriptstyle transfer} \\ J_E & \xrightarrow{\psi_E} & G_E^{ab} \end{array}$$

Relations Between Local and Global Class Field Theory

Let $F/\mathbb{Q}$ be a number field. Let $\bar{F}$ be a fixed algebraic closure of F. Let F^{ab} be the maximal abelian extension. Let $\mathfrak{p} \subset \mathcal{O}_F$ be a non-zero prime ideal. Let $\bar{F}_{\mathfrak{p}}$ be a fixed algebraic closure of $F_{\mathfrak{p}}$. Fix an embedding $\bar{F} \longrightarrow \bar{F}_{\mathfrak{p}}$. Recall that this induces a continuous embedding $G_{F_{\mathfrak{p}}} \to G_F$. Hence this gives rise to an embedding $G_{F_{\mathfrak{p}}}^{ab} \to G_F^{ab}$. Observe that there is a natural injective homomorphism $i : F_{\mathfrak{p}}^* \longrightarrow J_F$ given by identity at $\mathfrak{p}$ and 1 elsewhere. The compatibility between local and global class field theory is expressed by the following commutative diagram:

$$\begin{array}{ccc} F_{\mathfrak{p}}^* & \xrightarrow{\theta_{F_{\mathfrak{p}}}} & G_{F_{\mathfrak{p}}}^{ab} \\ \downarrow i & & \downarrow \\ J_F & \xrightarrow{\psi_F} & G_F^{ab} \end{array}$$

At the level of Weil groups, for every non-trivial non-archimedean place $\mathfrak{p} \subset \mathcal{O}_F$ there is an embedding

$$W_{F_v} \longrightarrow W_F$$

This induces the natural commutative diagram:

$$\begin{array}{ccc} F_{\mathfrak{p}}^* & \xrightarrow{\theta_{F_{\mathfrak{p}}}} & W_{F_{\mathfrak{p}}}^{ab} \\ \downarrow i & & \downarrow \\ C_F & \xrightarrow{\psi_F} & W_F^{ab} \end{array}$$

Observe that because $W_F^{ab} \cong C_F$, W_F has an "archimedean component" not shared with G_F. Recall that there is a surjective topological homomorphism: $W_F \longrightarrow G_F$. The kernel contains all the archimedean stuff. One should not ignore this. In fact for v an archimedean place of F, there is a version of the Weil group W_{F_v}. Remember that F_v is either $\mathbb{R}$ or $\mathbb{C}$ so there are only two choices. In the case $F_v = \mathbb{C}$ it turns out that $W_{\mathbb{C}} = \mathbb{C}^*$. In the case $F_v = \mathbb{R}$, $W_{\mathbb{R}}$ is an extension of $\mathbb{C}^*$ by the cyclic group of order 2. These look quite mysterious. Miraculously these two groups strictly control the behaviour of the representation theory of reductive lie groups. This is the subject of the local archimedean Langlands correspondence which we shall not talk about further.

Hecke Characters

For a moment let F be a finite extension of $\mathbb{Q}_p$. Recall that local class field theory could be interpreted as a natural bijection between one dimensional continuous representations of W_F and $GL_1(F)$. Can we do something similar for global class field theory?

Let $F/\mathbb{Q}$ be a number field. Let $\bar{F}$ be a fixed algebraic closure of F. Let F^{ab} be the maximal abelian extension. Observe that $GL_1(\mathbb{A}_F) = J_F$.

Definition. *A Hecke character of F is a continuous homomorphism (for the usual topology on $\mathbb{C}$)*

$$C_F = GL_1(F)\backslash GL_1(\mathbb{A}_F) \longrightarrow \mathbb{C}^*.$$

Let $\rho : G_F \longrightarrow \mathbb{C}^*$ be a continuous character. Note that because G_F is totally disconnected we may as well take the discrete topology on $\mathbb{C}^*$. As G_F is compact we deduce that ρ must

have finite image. Moreover ρ must factor through the quotient G_F^{ab}. Pre-composing with the global reciprocity map $\psi_F : C_F \longrightarrow G_F^{ab}$ we get a Hecke character naturally associated to ρ. We say a Hecke Character is of finite order if it's image in $\mathbb{C}^*$ is finite. This establishes a natural bijection:

$$\{ \text{ Hecke characters of } F \text{ of finite order } \}$$

$$\updownarrow$$

$$\{ \text{ One dimensional continous complex representations of } G_F \}$$

What happens if we talk another field than $\mathbb{C}$? Recall that $G_{\mathbb{Q}}^{ab} \cong \prod_{p\ prime} \mathbb{Z}_p^*$. Hence there is a natural continuous (for the p-adic topology) group homomorphism:

$$\chi_p : G_{\mathbb{Q}} \longrightarrow G_{\mathbb{Q}}^{ab} \longrightarrow \mathbb{Z}_p^*.$$

If we fix an algebraic closure $\bar{\mathbb{Q}}_p$, then χ_p may be naturally interpreted as a continuous character:

$$\chi_p : G_{\mathbb{Q}} \longrightarrow \bar{\mathbb{Q}}_p^*.$$

We call χ_p the p-adic cyclotomic character. If we fix an algebraic closure $\bar{\mathbb{Q}}$ and take $F/\mathbb{Q}$ a number field contained in $\bar{\mathbb{Q}}$ then there is a natural embedding $\phi : G_F \longrightarrow G_{\mathbb{Q}}$. Hence there is a natural notion of the p-adic cyclotomic character of G_F, after pre-composing χ_p with ϕ. By a standard abuse of notation we'll also denote it by χ_p. There is a very curious link between these p-adic character and Hecke characters as we'll see next time.

Number Theory

Alexander Paulin

November 30, 2009

Lecture 13

Hecke Characters

Let $F/\mathbb{Q}$ be a number field. Let $\bar{F}$ be a fixed algebraic closure of F. Let F^{ab} be the maximal abelian extension. Recall that Global class field theory gives natural continuous surjective reciprocity homomorphism:

$$\psi_F : GL_1(F)\backslash GL_1(\mathbb{A}_F) \longrightarrow Gal(F^{ab}/F).$$

The kernel is connected component containing the identity. This gives us a reasonably explicit understanding of all finite Abelian extensions of F contained in $\bar{F}$. Motivated by this we introduce the following fundamental definition.

Definition. *A Hecke character of F is a continuous homomorphism (for the usual topology on $\mathbb{C}$)*

$$GL_1(F)\backslash GL_1(\mathbb{A}_F) \longrightarrow \mathbb{C}^*.$$

We saw that if $\rho : G_F \longrightarrow \mathbb{C}^*$ is continuous character, then ρ has finite image and factors through $Gal(\bar{F}/F)$. Pre-composing with ψ_F yields a Hecke character of F with finite image. Hence the reciprocity map induces a canonical bijection:

$$\{ \text{ Hecke characters of } F \text{ of finite order } \}$$

$$\updownarrow$$

$$\{ \text{ One dimensional continous complex representations of } G_F \ \}$$

If we use the Global Weil group W_F instead then there is a tight fit:

$$\{ \text{ Hecke characters of } F\}$$

$$\updownarrow$$

$$1$$

{ One dimensional continous complex representations of W_F }

There are many more Hecke characters than those of finite order. Recall that given $x \in GL_1(\mathbb{A}_F)$, we may define $||x|| = \prod_v |x_v|_v$. This defines a continuous character of $GL_1(\mathbb{A}_F)$. The product formula tells us that $||x|| = 1$ for all $x \in F^*$. Hence $||.||$ defines a Hecke character on F. Observe that it is clearly not of finite order For example, for $F = \mathbb{Q}$, recall that

$$GL_1(\mathbb{Q})\backslash GL_1(\mathbb{A}_\mathbb{Q}) \cong \mathbb{R}_{>0} \times \prod_{p\ prime} \mathbb{Z}_p^*.$$

We freely pass between these two perspectives. Let $x \in \mathbb{R}_{>0} \times \prod_{p\ prime} \mathbb{Z}_p^*$. Then $||x|| = x_\infty$. The connected component containing the identity is topologically isomorphic to $\mathbb{R}_{>0}$. All continuous complex characters of $\mathbb{R}_{>0}$ are of the form

$$\begin{aligned} |.|^s : \mathbb{R}_{>0} &\longrightarrow \mathbb{C}^* \\ a &\longrightarrow a^s \end{aligned}$$

for a unique $s \in \mathbb{C}$. From this we see that a Hecke character is uniquely of the form

$$(\chi, s)(x) = \chi(x)||x||^s,$$

where χ is a finite order character, $s \in \mathbb{C}$.

In general it is more difficult to give such an explicit description because the connected component on the identity can be very complicated. Hence finite order Hecke Characters correspond to $(\chi, 0)$ in the above notation. It would be reasonable to assume that this was as far as the relation between Hecke characters and characters of G_F can be pushed. If a Hecke character doesn't vanish on the connected component containing the identity how can it possibly give a character of G_F? You are correct - it won't give a character over $\mathbb{C}$. However there is a natural class of characters of G_F taking values in p-adic fields.

The Cyclotomic Character

There was no inherent reason that we chose to take characters in $\mathbb{C}$. Recall that $\mathbb{C}$ is just the algebraic closure of the archimedean completions of $\mathbb{Q}$. Why don't we do the same for a non-archimedean completion. The fist issue to address is what the correct analogue of $\mathbb{C}$ should be. Let $p \in \mathbb{Z}$ be a prime . Let us fix an algebraic closure $\bar{\mathbb{Q}}_p$. One would naively hope that $\bar{\mathbb{Q}}_p$ would be the correct avatar of $\mathbb{C}$. Unfortunately one of the key properties of $\mathbb{C}$, completeness, is not shared by $\bar{\mathbb{Q}}_p$. Let $\mathbb{C}_p$ be the completion of $\bar{\mathbb{Q}}_p$ with respect to the canonical metric. It is a fact the $\mathbb{C}_p$ is algebraically closed. This is the p-adic equivalent of $\mathbb{C}$.

Definition. *A p-adic Hecke character of F is a continuous homomorphism (for the canonical topology on $\mathbb{C}_p$)*

$$GL_1(F)\backslash GL_1(\mathbb{A}_F) \longrightarrow \mathbb{C}_p^*.$$

Recall that in the classical case the subtle behavior of the Hecke character occurred at the archimedean places. This was because of the incompatibility between the p-adic and complex topology. In this case the interesting behavior will occur at finite places dividing p. In particular because $\mathbb{C}_p$ is totally disconnected we know that a p-adic Hecke character must vanish on the connected component containing the identity. Thus there is a natural bijection:

$$\{ \text{ } p\text{-adic Hecke characters of } F \text{ } \}$$

$$\updownarrow$$

$$\{ \text{ one dimensional continuous representations of } G_F \text{ on a one dimensional } \mathbb{C}_p\text{-vector space } \}$$

Observe that there is a much tighter fit between p-adic Hecke characters and p-adic Galois characters. This shouldn't surprise us - G_F not very archimdean.

For simplicity let us restrict to the case $F = \mathbb{Q}$ again.

$$GL_1(\mathbb{Q})\backslash GL_1(\mathbb{A}_\mathbb{Q}) \cong \mathbb{R}_{>0} \times \prod_{p \text{ } prime} \mathbb{Z}_p^*.$$

Because $\mathbb{C}_p$ is totally disconnected and $\mathbb{R}_{>0}$ is path connected can see that any p-adic Hecke character is determined by its behaviour in the non-archimdean component $\prod_{p \text{ } prime} \mathbb{Z}_p^*$. The character $||.||$ projected onto the archimedean component. Similarly we can define the projection χ_p onto the p-adic component. This gives a p-adic Hecke character

$$\chi_p : GL_1(F)\backslash GL_1(\mathbb{A}_F) \longrightarrow \mathbb{Z}_p^* \subset \mathbb{C}_p^*.$$

By the above correspondence we get the natural continuous character:

$$\chi_p : G_\mathbb{Q} \longrightarrow G_\mathbb{Q}^{ab} \longrightarrow \mathbb{Z}_p^* \subset \mathbb{C}_p^*.$$

χ_p is called the p-adic cyclotomic character. Note that χ_p is clearly not of finite order. If we fix an algebraic closure $\bar{\mathbb{Q}}$ and take $F/\mathbb{Q}$ a number field contained in $\bar{\mathbb{Q}}$ then there is a natural embedding $\phi : G_F \longrightarrow G_\mathbb{Q}$. Hence there is a natural notion of the p-adic cyclotomic character of G_F, after pre-composing χ_p with ϕ. By a standard abuse of notation we'll also denote it by χ_p. As in the classical case every p-adic Hecke character of $\mathbb{Q}$ can be expressed by

$$(\chi, \kappa)(x) = \chi(x)\kappa(\chi_p(x_p)),$$

where χ is a finite order character and κ is a continuous $\mathbb{C}_p^*$ valued character of $\mathbb{Z}_p^*$. In this case this representation is not unique because κ could be finite order without being trivial.

Note that there is nothing special about p here. We could have chosen any prime.

Restrict to the case $F = \mathbb{Q}$. Fix embedding $\bar{\mathbb{Q}} \subset \mathbb{C}$ and $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_p$. This established a natural bijection:

$$\{ \text{ Hecke characters of } F \text{ of finite order } \}$$

$$\updownarrow$$

$$\{ p\text{-adic Hecke characters of } F \text{ of finite order } \}$$

Assume that we have a Hecke character of $\mathbb{Q}$, given by (χ, k), such that χ is or finite order and $k \in \mathbb{Z}$. Such Hecke characters are called arithmetic. Similarly we define the arithmetic p-adic Hecke characters to be the ones of form (χ, k) where χ is a finite order p-adic Hecke character and $k \in \mathbb{Z}$ denotes the homomorphism: $K : \mathbb{Z}_p^* \to \mathbb{C}_p^*, z \to z^k$. Arithmetic p-adic Hecke characters correspond to continuous characters $\phi : G_{\mathbb{Q}} \to \mathbb{C}_p^*$ such that $\phi\chi_p^k$ is of finite order for some $k \in \mathbb{Z}$. We call such characters potentially semi-stable. I'll explain why later.

Hence we have established a natural series of bijections bijection:

$$\{ \text{ Arithmetic Hecke Characters of } \mathbb{Q} \}$$

$$\updownarrow$$

$$\{ \text{ Arithmetic } p\text{-adic Hecke characters of } \mathbb{Q} \}$$

$$\updownarrow$$

$$\{ p\text{-adic potentially semi-stable characters of } G_{\mathbb{Q}} \}$$

Number Theory

Alexander Paulin

November 30, 2009

Lecture 14

Last time we saw a natural bijection between three sets:

$$\{ \text{ Arithmetic Hecke Characters of } \mathbb{Q} \ \}$$

$$\updownarrow$$

$$\{ \text{ Arithmetic } p\text{-adic Hecke characters of } \mathbb{Q} \ \}$$

$$\updownarrow$$

$$\{ \ p\text{-adic potentially semi-stable characters of } G_{\mathbb{Q}} \ \}$$

We focused on the $F = \mathbb{Q}$ case because we have a very explicit description of $GL_1(\mathbb{Q})\backslash GL_1(\mathbb{A}_F)$. We can extend this to an arbitrary number field as follows:

Let $\sigma : F \to \mathbb{C}$ be an embedding. If v is the infinite place corresponding to σ then there is an induced embedding $\sigma_v : F_v \to \mathbb{C}$. Recall that if v is real is corresponds to a unique such σ. If v is complex it corresponds to a unique complex conjugate pair. We say that a Hecke character χ over F is arithmetic if there exist integers n_σ for each embedding such that

$$\chi|_{(\prod_{v|\infty} F_v)^o}(x) \prod_{\sigma : F \to \mathbb{C}} \sigma_v(x_v)^{n_\sigma}.$$

The possible n_σ which can occur is actually very restricted.

Definition. *A number field $M/\mathbb{Q}$ is totally real if all its archimedean completions are isomorphic to $\mathbb{R}$. A number field $K/\mathbb{Q}$ is totally imaginary if all its archimedean completions are isomorphic to $\mathbb{C}$. A number field $L/\mathbb{Q}$ is a CM field if it is totally imaginary but contains a subfield of index 2 which is totally real.*

The following is a result of Weil.

Proposition. *Suppose that χ is an arithmetic Hecke character of F then either*

1. *If F does not contain a CM field then n_σ are independent of σ.*

2. *If F contains a CM field L, then $\exists w \in \mathbb{Z}$ and integers m_α $\forall$ embeddings $\alpha : L \to \mathbb{C}$ such that (1) $m_\alpha + m_{\bar{\alpha}} = w$ independent of α and (2) $n_\sigma = m_{\sigma|_L}$. Here $\bar{\alpha}$ denotes the complex conjugate embedding of α.*

This greatly restricts the possible n_σ which can occur.

Let us fix a prime number $p \in \mathbb{N}$. In a similar way we can define an arithmetic p-adic Hecke character of F as follows. For each place v of F dividing p we have an embedding $\sigma_v : F_v \to \mathbb{C}_p$. A p-adic Hecke character χ, is arithmetic if there exist integers n_v such that

$$\chi|_{\prod_{v|p} F_v}(x) = \Gamma(x) \prod_{v|p} \sigma_v(x_v)^{n_v}.$$

where Γ is a p-adic Hecke character with finitie image.

Let χ be an arithmetic (classical) Hecke character of F. We define

$$\begin{array}{rcl} \chi_0 : GL_1(\mathbb{A}_F) & \longrightarrow & \mathbb{C}^* \\ x & \longrightarrow & \chi(x) \prod_{\sigma : F \to \mathbb{C}} \sigma_v(x_v)^{-n_\sigma} \end{array}$$

Observe that χ_0 is naturally a continuous homomorphism on $GL_1(\mathbb{A}_F)/(\prod_{v|\infty} F_v)^o$. It is no longer invariant by $GL_1(F)$.

It is a fact that $E_\chi \subset \mathbb{C}$ the field generated by $\mathbb{Q}$ and the image of χ_0 is a number field. Let us fix a prime number $p \in \mathbb{N}$ and λ a place of E_χ lying over p. Let $E_{\chi,\lambda}$ denote the completion and $F_p = \prod_{v|p} F_v$. It is a fact that the map

$$\begin{array}{rcl} F^* & \longrightarrow & E_\chi^* \\ x & \longrightarrow & \prod_{\sigma : F \to \mathbb{C}} \sigma(x)^{n_\sigma} \end{array}$$

extends to a unique continuous homomorphism $\phi_p : F_p^* \to E_{\chi,\lambda}^*$. Hence we may define the continuous

$$\begin{array}{rcl} \chi_0\phi_p : GL_1(\mathbb{A}_F) & \longrightarrow & E_{\chi,\lambda}^* \\ x & \longrightarrow & \chi_0(x)\phi_p(x_p) \end{array}$$

where x_p is projection of x onto F_p. Note that $\chi_0\phi_p$ is continuous (with respect to the canonical topology of $E_{\chi,\lambda}$) and by construction it contains $F^*(\prod_{v|\infty} F_v)^o$ Note that after fixing embeddings $E\chi \subset \bar{\mathbb{Q}}$ and $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_p$ it naturally gives rise to an arithmetic p-adic Hecke character. Thus observe that it must therefor correspond to a continuous character

$$\chi_\lambda^G : G_F \to E_{\chi,\lambda}^* \subset \mathbb{C}_p^*.$$

The characters which occur in this way can be characterized in purely Galois theoretic terms. From this perspective they are potentially semi-stable, a notion we do not make precise. It is somehow related to Geometry. Hence we have established the natural bijections:

$$\{ \text{ Arithmetic Hecke Characters of } F \ \}$$

$$\updownarrow$$

$$\{ \text{ Arithmetic } p\text{-adic Hecke characters of } F \ \}$$

$$\updownarrow$$

$$\{ \ p\text{-adic potentially semi-stable characters of } G_F \ \}$$

Remember p was chosen freely. An arithmetic Hecke characters of F gives rise to a whole system of one dimensional continuous p-adic representations of G_F. There is a technical sense in which they are compatible, defined purely Galois theoretically. We will return to these issues later in the course. Note that given a p-adic Hecke character on F we always get a p-adic Galois character. It is only when it is arithmetic does it fit into a compatible system of l-adic Galois characters as l varies over all primes.

In a sense, this is the correct way of viewing the main theorem of Global Class Field Theory. Why? The main reason is that this gives a clear hint as to how the generalise to higher dimensions. It also makes it clear that to understand G_F we are going to have to study it continuous representations on p-adic vector spaces.

1 The Local Langlands Correspondence

Here is a powerful general philosophy:

Understanding a Group is the same as understanding it's category of representations

This is intentionally vague. What do we mean by representations? Classically a representation of a group G is just a linear action on a vector space. In a broader sense a representation of a group is some way that it naturally appears in another area of mathematics. As we shall see, a very common mechanism why which this occurs is through the classical concept. To truly understand the category of representations means that we truly understand how the group permeates mathematics as a whole. We've already seen this above. G_F is somehow manifesting itself in $GL_1(F)\backslash GL_1(\mathbb{A}_F)$ via it's one dimensional representations. This observation is deep - it forms the backbone of Langland's higher dimensional generalization of Local and Global Class Field theory.

As above let $F/\mathbb{Q}$ be a number field. Fix $p \in \mathbb{N}$ a prime number and let $K/\mathbb{Q}_p$ be a finite extension. Let V be a finite dimensional K-vector space. Let ρ be a continuous K-linear action of G_F on V. In other words, if $dim_K(V) = n$, then after fixing a basis we get the continuous homomorphism:

$$\rho : G_F \longrightarrow GL_n(K).$$

For $n = 1$ this is precisely the type of object we have been considering above. For the moment we shall forgo trying to understand what the correct higher dimensional reformulation of Global Class Field theory should be. Instead we will try and understand these objects in abstraction. Let $l \in \mathbb{N}$ be a prime number. Let v be a place of F dividing l. Let $\bar{F}_v$ be an algebraic closure and fix an embedding $\bar{F} \subset \bar{F}_v$. This induces an embedding $G_{F_v} \subset G_F$. We have already seen that to study G_F it was worthwhile restricting to such G_{F_v}. This made problems more tractable because we have more of a handle on the structure of G_{F_v}. Note that we may restrict ρ to give

$$\rho_v : G_{F_v} \longrightarrow GL_n(K).$$

Note that there are two quite different situations which can occur. Either $l = p$ or $l \neq p$. The former of these is much more complicated because the topologies on either side are both pretty p-adic and hence can interact in subtle ways. The later situation, although still difficult, is much easier. The classical Local Langlands correspondence for GL_n is a classification of such representations for $l \neq p$.

Number Theory

Alexander Paulin

November 23, 2009

Lecture 15

Let $p, l \in \mathbb{N}$ be two distinct prime numbers. Let $F/\mathbb{Q}_p$ and $K/\mathbb{Q}_l$ be finite extensions ad fix $\bar{F}$ an algebraic closure. Let V be a finite dimensional K-vector space. Let ρ be a continuous K-linear representation of G_F on V . In other words, if $dim_K(V) = n$, then after fixing a basis we get the continuous homomorphism:

$$\rho : G_F \longrightarrow GL_n(K).$$

We would like to somehow classify such representations independently. The first step will be to put ρ into a more manageble form. Recall that Local Class Field theory worked between if we restricted our attention to the Weil group $W_F \subset G_F$, i.e. $W_F^{ab} \cong GL_1(F)$. Because the inclusion is continuous we know that $\rho|_{W_F}$ is still continuous. Recall that we did not give W_F the subspace topology. We gave $I_F \subset W_F$ the induced subspace topology then gave W_F the disjoint union topology. In particular, W_F was not compact. However, W_F is dense in G_F, hence ρ is determined by $\rho|_{W_F}$, so we lose nothing by restriction to W_F. From now on let ρ be a continuous K-linear representation of W_F on V.

This broadens our study. This is apparent even in the case $n = 1$. Recall that there is a canonical isomorphism $W_F/I_F \cong \mathbb{Z}$. Let $Frob_F \in W_F$ be a lift of frobenius. $Frob_F$ is only well defined up to a multiple of I_F. Given any $\alpha \in GL_1(K)$ there is a unique one dimensional continuous representation

$$\rho_\alpha : W_F \longrightarrow GL_1(K),$$

which is trivial on I_K and sends $Frob_F$ to α. Clearly if $|\alpha| \neq 1$ then the image is unbounded and in particular is not compact in $GL_1(K)$. However, by compactness, any continuous character of G_F into $GL_1(K)$, must have image contained in $\mathcal{O}_K^*$. Hence there are many more such representations of W_F, than of G_F.

Let us return to the general case. The topology of W_F is completely controlled by $I_F \subset W_F$. Recall that $I_F = Gal(\bar{F}/F^{nr})$, where $F^{nr} \subset \bar{F}$ is the maximal unramified extension of F in $\bar{F}$. In particular it is compact. This implies that $\rho(I_F) \subset GL_n(K)$ is compact. All compact subgroups of $GL_n(K)$ are conjugate to $GL_n(\mathcal{O}_K)$. Hence after changing the basis we may assume that $\rho(I_F) \subset GL_n(\mathcal{O}_K)$. Let $\pi \subset \mathcal{O}_K$ be a uniformiser. The subgroup

$I_n + \pi^2 M_n(\mathcal{O}_K) \subset GL_n(\mathcal{O}_K)$ is of finite index. After restricting ρ to I_F the inverse image if $I_n + \pi^2 M_n(\mathcal{O}_K)$ is an open normal subgroup of I_F. By the Fundamental theorem of Galois theory there is a finite extension E'/F^{nr} such that $\rho(Gal(\bar{F}/E')) \subset I_n + \pi^2 M_n(\mathcal{O}_K)$. Let E be a finite extension of F containing the generators of E' over F^{nr}. Then $E' \subset E^{nr}$ and thus $\rho(I_E) \subset I_n + \pi^2 M_n(\mathcal{O}_K)$. Observe that by completeness and the fact that the residue characteristic of K is l, $\mathcal{O}_K$ is a pro-l group. Hence $I_n + \pi^2 M_n(\mathcal{O}_K)$ is a pro-l group. Let $E^{tr} \subset \bar{F}$ be the maximal tamely ramified extension of E. Recall that $E^{nr} \subset E^{tr}$ and $Gal(\bar{F}/E^{tr})$ is a pro-p group. Note that any continuous homomorphism from a pro-p group to a finite l-group must be trivial, as $l \neq p$. Thus any continuous homomorphism from a pro-p group to a pro-l group must be trivial for $l \neq p$. Hence $\rho(Gal(\bar{F}/E^{tr})) = I_n$ and ρ restricted to I_E must factor through $Gal(E^{tr}/E^{nr})$. Recall that there is a (non-canonical) topological isomorphism

$$Gal(E^{tr}/E^{nr}) \cong \prod_{q \neq p} \mathbb{Z}_q.$$

Observe that this gives a continuous homomorphism $t : I_E \to \mathbb{Z}_l$ after projecting onto the l^{th} component. For the same reason as above $\rho|_{Gal(E^{tr}/E^{nr})}$ is completely determined by its behavior on the $\mathbb{Z}_l$ component. Recall that $\mathbb{Z} \subset \mathbb{Z}_l$ is dense, thus by continuity, $\rho|_{Gal(E^{tr}/E^{nr})}$ is completely determined by the image of

$$1 \in \mathbb{Z} \subset \mathbb{Z}_l \subset \prod_{q \neq p} \mathbb{Z}_q \cong Gal(E^{tr}/E^{nr}).$$

Let us write $\rho(1) := U \subset I_n + \pi^2 M_n(\mathcal{O}_K)$. Note that given $A \in I_n + \pi^2 M_n(\mathcal{O}_K)$ and $\beta \in \mathbb{Z}_l$ it makes sense to talk about A^β because the coefficients of the binomial expansion converge. Hence we have shown that given $\sigma \in I_E, \rho(\sigma) = U^{t(\sigma)}$. There is a natural continuous homomorphism from $I_n + \pi^2 M_n(\mathcal{O}_K)$ to $M_n(\mathcal{O}_K)$ defined by the logarithmic power series, i.e. for $A \in \pi^2 M_n(\mathcal{O}_K)$ we define

$$log(I_n + A) = A - \frac{A^2}{2} + \frac{A^3}{3} - \frac{A^4}{4} + \frac{A^5}{5} + \cdots$$

This converges because of the condition on the coefficients. There is a partial inverse map exp defined at the level of power series in the usual way. The reason it is partial is that it will not always converge because the denominators $m!$ may count against us l-adically. However given and $A \in \pi^2 M_n(\mathcal{O}_K)$, exp makes sense on $log(I_n + A)$ and we have $exp(log(I_n + A)) = I_n + A$. Let $N = log(U)$. Hence given $\sigma \in I_E$, $\rho(\sigma) = exp(t(\sigma)N) \subset I_n + \pi^2 M_n(\mathcal{O}_K)$.

Let $q \in \mathbb{N}$ denote the cardinality of the residue field of F. Recall that if $\sigma \in Gal(F^{tr}/F^{nr})$ and $\Phi \in W_F$ is a lift of frobenius then $\Phi\sigma\Phi^{-1} = \sigma^q$. Hence $\rho(\Phi)U\rho(\Phi)^{-1} = U^q$. Hence $\rho(\Phi)exp(U)\rho(\Phi)^{-1} = exp(\rho(\Phi)U\rho(\Phi)^{-1}) = exp(U^q) = qN$. We deduce that N is nilpotent. Let $||.|| : W_F \to \mathbb{Q}^*$ be the character which is trivial on I_F and sends Φ to q. By the above we know that

$$\rho(\sigma)N\rho(\sigma)^{-1} = ||\sigma||N, \ \ \forall \sigma \in W_F.$$

There is a unique character additive character $\lambda : I_F \to \mathbb{Q}_p$ such that $\lambda|_{I_E} = t$. Indeed all such additive characters are unique to be scalar. We define the representation ρ_0 given by

$$\rho_0(\Phi^m u) = \rho(\Phi^m u) exp(-\lambda(u)N), \ \ \forall m \in \mathbb{Z}\ u \in I_F.$$

By construction this representation is trivial on the finite index subgroup $I_E \subset I_F$. Hence

$$\rho_0 : W_F \longrightarrow GL_n(K)$$

is continuous with respect to the discrete topology on K. Essentially what we've shown is that when $l \neq p$, ρ is not far away from being continuous with respect to the discrete topology on K. The only thing preventing it is N, which we call the *monodromy operator*. This motivates the following definition:

Definition. *A Weil-Deligne representation of W_F over K is a pair (ρ_0, N), where*

1. *$\rho_0 : W_F \longrightarrow GL_n(K)$ is a continuous homomorphism with respect to the discrete topology on K.*
2. *$N \in M_n(K)$ is nilpotent and $\rho_0(\sigma) N \rho_0(\sigma)^{-1} = ||\sigma|| N$ for all $\sigma \in W_F$.*

We call N the monodromy operator as above. There is an obvious concept of a morphism between Weil-Deligne representations. What we have shown is that a ρ of the above form naturally gives rise to a Weil-Deligne representation. Somehow the monodromy operator is a measure of how far ρ is from being continuous with respect to the discrete topology on K. Conversely given a Weil-Deligne representation (ρ_0, N) we may construct a representation continuous (with respect to the l-adic topology on K) representation

$$\begin{aligned} \rho : W_F &\longrightarrow GL_n(K) \\ \Phi u &\longrightarrow \rho(\Phi u) exp(\lambda(u)N) \end{aligned}$$

where $\Phi \in W_F$ is a lift of frobenius and $u \in I_F$. The isomorphism class of this representation is independent of all choices. Hence we have established

Grothendieck's Abstract Monodromy Theorem. *There are is a natural bijection:*

{ *Isomorphism classes of n-dimensional Weil-Deligne representations of W_F over K* }

$$\updownarrow$$

{ *Isomorphism classes of continuous (w.r.t l-adic topology on K) n-dimensional K-linear representations of W_F* }

The bijection is given by the above construction. This makes things easier because we only have to worry about one topology. We say that a Weil-Deligne representation is Frobenius semi-simple if the underlying Weil representation is semi-simple, i.e. the direct sum of irreducible representations.

Number Theory

Alexander Paulin

November 23, 2009

Lecture 16

Let $p, l \in \mathbb{N}$ be two distinct prime numbers. Let $F/\mathbb{Q}_p$ and $K/\mathbb{Q}_l$ be finite extensions and fix $\bar{F}$ an algebraic closure. Let q denote the cardinality of the residue field. Let V be a finite dimensional K-vector space. Let ρ be a continuous K-linear representation of W_F on V . In other words, if $dim_K(V) = n$, then after fixing a basis we get the continuous homomorphism:

$$\rho : W_F \longrightarrow GL_n(K).$$

Recall that because l and p are distinct, the topology on W_F and $GL_n(K)$ are fairly incompatible. We saw that the only obstruction to ρ being continuous for the discrete topology on K was a *monodromy* operator $N \in M_n(K)$. More precisely, if we fix a continuous non-trival additive character $\lambda : I_F \to \mathbb{Q}_p$ then there is a nilpotent matrix $N \in M_n(K)$ and $c \in \mathbb{Q}_p$ such that there exists a finite extension E/F (in $\bar{F}$) such that

$$\rho(u) = exp(c\lambda(u)N) \ \forall u \in I_E.$$

The $c \in \mathbb{Q}_p$ is chosen such that $c\lambda(I_E) = \mathbb{Z}_p$. Moreover if $||.|| : W_F \to \mathbb{Q}^*$ is the character which is trivial on I_F and sends a lift of frobenius to q then

$$\rho(\sigma)N\rho(\sigma)^{-1} = ||\sigma||N \ \forall \sigma \in W_F.$$

This motivates the important definition:

Definition. *A Weil-Deligne representation of W_F over K is a pair (ρ_0, N), where*

1. *$\rho_0 : W_F \longrightarrow GL_n(K)$ is a continuous homomorphism with respect to the discrete topology on K.*
2. *$N \in M_n(K)$ is nilpotent and $\rho_0(\sigma)N\rho_0(\sigma)^{-1} = ||\sigma||N$ for all $\sigma \in W_F$.*

Remarks. *There is an obvious concept of morphisms between Weil-Deligne representations. We may actually interpret a Weil-Deligne representation as representation (over K) of a cleverly constructed group scheme which is the semi-direct product of W_F and $\mathbb{G}_m$. For more details see the bottom of page 19 of Tate's "Number Theoretic Background" article in the Corvallis proceedings.*

If $\Phi \in W_F$ is a lift of Frobenius then the map

$$\begin{aligned} \rho : W_F &\longrightarrow GL_n(K) \\ \Phi u &\longrightarrow \rho_0(\Phi u) exp(\lambda(u)N) \end{aligned}$$

Gives a continuous representation of W_F for the l-adic topology on K. It's isomorphism class is independent of the choice Φ and λ. This establishes

Grothendieck's Abstract Monodromy Theorem. *There are is a natural bijection:*

{ *Isomorphism classes of n-dimensional Weil-Deligne representations of* W_F *over* K }

$$\updownarrow$$

{ *Isomorphism classes of continuous (w.r.t l-adic topology on* K*) n-dimensional* K*-linear representations of* W_F }

Remarks.

1. *We say that* (ρ_0, N)*, a Weil-Deligne representation, is* Φ*-semisimple if the underlying representation of* W_F *is semisimple, i.e. the direct sum of (algebraically) irreducible representations of* W_F*. This is equivalent to* $\rho_0(\Phi) \in GL_n(K)$ *being semisimple, i.e. diagonalizable. It is these representations which will be the focus of the Local Langlands correspondence.*

2. *We say that* ρ *is unramified if it is trivial on* I_F*. Clearly such a representation has trivial monodromy. Because* $W_F/I_F \cong \mathbb{Z}$ *we know that unramified* Φ*-semisimple Weil-Deligne representations correspond to semisimple conjugacy classes in* $GL_n(K)$*, i.e. conjugacy classes containing diagonal matrices.*

3. *Note that in the case* $n = 1$ *the monodromy operator is a nilpotent operator on a 1-dimensional* K *vector space, hence it must be trivial. Thus non-trivial monodromy only arrises in higher dimensions.*

4. *By definition, if* (ρ_0, N) *is Weil-Deligne representation over* K *then* $ker(N) \subset V$ *is fixed by* ρ_0*. Hence* (ρ_0, N) *is irreducible* $\iff$ $N = 0$ *and* ρ_0 *is irreducible. More generally, if* ρ*, the* l*-adic representation attached to* (ρ_0, N) *is semisimple then* $N = 0$*.*

5. *Here is an important example, which we call* $Sp(n)$*:*

$$V = Ke_0 + Ke_1 + \cdots + Ke_{n-1}$$

$$\rho_0(\sigma)e_i = ||\sigma||^i e_i \ \forall \sigma \in W_F, \ i \in \{0, 1, \cdots n-1\}$$

$$Ne_i = e_{i+1} \ \forall \ i \in \{0, 1, \cdots n-2\}; \ Ne_{n-1} = 0.$$

We say that a Weil-Deligne representation is indecomposable if it cannot be expressed as the direct sum of two non-trivial sub Weil-Deligne representations. $Sp(n)$ is indecomposable. Moreover, all Φ-semisimple indecomposable Weil-Deligne representations are of the form $\rho' \otimes Sp(n)$ for some irreducible ρ'. Here the tensor product of two Weil-Deligne representations (ρ_1, N_1) and $(\rho_2, N_2$ is $(\rho_1 \otimes \rho_2, N_1 \otimes 1 + 1 \otimes N_2)$. Hence any Φ-semisimple Weil-Deligne Representation can be written as the direct sum of such indecomposable Weil-Deligne representations.

This gives one side of the Local Langlands Correspondence. What about the other.

Smooth Admissible Representations of $GL_n(F)$

Let us keep the notation of the previous paragraph. By switching to Weil-Deligne representations we have effectively removed the topological structure of K from the picture. There is no harm therefore in assuming that $K = \mathbb{C}$. Because $\mathbb{C} \cong \mathbb{C}_p$ as abstract field there is no real restriction in doing this. Recall that Local Class Field theory gave a natural bijection between 1-dimensional Weil-Deligne representations of W_F over $\mathbb{C}$ and complex 1-dimensional continuous representations of $GL_1(F)$. What should the corresponding objects be for n-dimensional Weil-Deligne representations for $n > 1$. An obvious guess is that it should somehow involve $GL_n(F)$. This is correct but what should we replace complex continuous characters with? Clearly it should be something to do with representation theory. For $n > 1$ the topological group $GL_n(F)$ is **not** Abelian. Recall that the irreducible representations of Abelian groups are one dimensional. This is spectacularly not the case in this situation. The correct objects to consider will in fact be **infinite** dimensional representations of $GL_n(F)$. Let V be a complex vector space, not necessarily finite dimensional. Let Π be a $\mathbb{C}$-linear representation of $GL_n(F)$ on V, i.e. a homomorphism $\Pi : GL_n(F) \to GL(V)$, We introduce two important restrictions on (Π, V).

Definition. *1. We say that (Π, V) is smooth if given $v \in \Pi$, $stab(v) \subset GL_n(F)$ is an open subgroup. Equivalently given $v \in \Pi$, the orbit map*

$$\begin{aligned} \phi_v : G &\longrightarrow V \\ g &\longrightarrow g(v) \end{aligned}$$

is locally constant.

2. We say that (Π, V) is admissible if given $K \subset GL_n(F)$, an open compact subgroup, V^K is a finite dimensional complex vector space.

3. We say that (Π, V) is irreducible if it is irreducible in the usual sense, i.e. contains no non-trivial $GL_n(F)$ subrepresentations.

The Local Langlands correspondence (non-Abelian Local Class Field theory) asserts the following remarkable result:

The Local Langlands Correspondence for GL_n

There is a natural bijection between the two sets

{ Isomorphism classes of n-dimensional Φ-semisimple Weil-Deligne representations of W_F over $\mathbb{C}$ }

$$\updownarrow$$

{ Isomorphism classes of irreducible smooth admissible representations of $GL_n(F)$ on a complex vector space }

Remarks.

1. *The operative word is natural. This is hard to define, but it involves attaching natural invariants to objects on both sides and demanding that they coincide. These invariants are complex analytic functions called local L and ϵ factors. To motivate their definition we need to understand the Global picture more.*

2. *This correspondence was proven in total generality by Richard Taylor and Michael Harris in 2000, using very sophisticated geometric techniques. In low dimensions it had been known since the 1970s . For $n = 2$ if had essentially been proven by hand by Langlands and Tunnel.- writing out both sides and matching them up.*

3. *The correspondence makes sense (and remains true) over any field K of characteristic zero.*

4. *There is a version of the correspondence when we replace GL_n with an arbitrary reductive algebraic group. In this case the it is not clear what the Weil-Deligne side should look like, but it can be made sense of. In this generality the correspondence is still a conjecture.*

Number Theory

Alexander Paulin

November 10, 2009

Lecture 17

Let F be a finite extension of $\mathbb{Q}_p$ and $n \in \mathbb{N}$. We wish to understand irreducible smooth admissible representations of $GL_n(F)$ on complex vector spaces. A complete classification of the isomorphism classes of such representations was given by Bernstein and Zelevinsky in the late 1970s. I'll partially describe their results.

Let V be a complex vector space and Π a $\mathbb{C}$-linear representation of $GL_n(F)$ on V, i.e. a group homomorphism $\Pi : GL_n(F) \to GL(V)$. Recall that Π is smooth if given $v \in \Pi$, $stab(v) \subset GL_n(F)$ is an open subgroup. Also recall that Π is admissible if given $K \subset GL_n(F)$ an open compact subgroup V^K is a finite dimensional complex vector space. Let the set of isomorphism classes of irreducible smooth admissible representation of $GL_n(F)$ be denoted $\mathcal{A}_n(F)$.

As every open subgroup of $GL_n(F)$ contains an open compact subgroup ($GL_n(F)$ is locally compact) Π is smooth if and only if

$$V = \bigcup_K V^K,$$

where K runs over all open compact subgroups of $GL_n(F)$.

Hecke Algebras

Let $(\Pi, V) \in \mathcal{A}_n(F)$ and $K \subset GL_n(F)$ be an open compact subgroup such that $V^K \neq \{0\}$. Let $\mathcal{H}(K\backslash GL_n(F)/K)$ be the set of compactly supported (zero off a compact set) K-bi-invariant $\mathbb{C}$-valued functions on $GL_n(F)$. The simplest example is $1_K \in \mathcal{H}(K\backslash GL_n(F)/K)$ which is 1 on K and 0 elsewhere. Recall that $GL_n(F)$ is a locally compact topological group. Hence it possesses a unique (up to scalar) left (and right) Haar measure. In fact $GL_n(F)$ is unimodular so these measures coincide. We normalise the Haar measure such that

$$\int_{GL_n(F)} 1_{GL_n(\mathcal{O}_F)} dg = 1.$$

Using this we may form the convolution product on $\mathcal{H}(K\backslash GL_n(F)/K)$ by

$$(f_1 * f_2)(h) = \int_{GL_n(F)} f_1(hg^{-1}) f_2(g) dg,$$

where $f_1, f_2 \in \mathcal{H}(K\backslash GL_n(F)/K)$ and $h \in GL_n(F)$. This integral is not so frightening as it is really just a finite sum as we'll see below. This naturally makes $\mathcal{H}(K\backslash GL_n(F)/K)$ an associative $\mathbb{C}$-algebra. If

$$vol(K) = \int_{GL_n(F)} 1_K dg,$$

then $e_K := (vol(K))^{-1} 1_K \in \mathcal{H}(K\backslash GL_n(F)/K)$ is a unit element in $\mathcal{H}(K\backslash GL_n(F)/K)$. We call $\mathcal{H}(K\backslash GL_n(F)/K)$ the Hecke algebra at K of $GL_n(F)$.

If $K' \subset K$ are two open compact subgroups then there is a natural inclusion $\mathcal{H}(K\backslash GL_n(F)/K) \subset \mathcal{H}(K'\backslash GL_n(F)/K')$. Observe that this inclusion is an embedding of rings (considered without unit). The union of all such spaces within the set of all measurable functions on $GL_n(F)$ gives

$$\mathcal{H}(GL_n(F)) := \bigcup_K \mathcal{H}(K\backslash GL_n(F)/K),$$

where K runs over all open compact subgroups of $GL_n(F)$. The space $\mathcal{H}(GL_n(F))$ is exactly the locally constant, compactly supported $\mathbb{C}$-valued functions on $GL_n(F)$. This is the full Hecke Algebra of $GL_n(F)$. If naturally has a convolution product as above, except this makes it an associate $\mathbb{C}$-algebra without unit.

Why have we introduced this algebra? Let $(\Pi, V) \in \mathcal{A}_n(F)$. Recall that

$$V = \bigcup_K V^K,$$

where K runs over all open compact subgroups of $GL_n(F)$. There is a natural action of $\mathcal{H}(K\backslash GL_n(F)/K)$ on V^K given by the integral

$$f(v) := \int_{Gl_n(F)} f(g) v dg,$$

where $f \in \mathcal{H}(K\backslash GL_n(F)/K)$ and $v \in V$. This integral is not really so bad - it's just a finite sum again. To make things more concrete let's do an example. Let $\alpha \in GL_n(F)$. Let $1_{K\alpha K} \in \mathcal{H}(K\backslash GL_n(F)/K)$, denote the function which takes the value 1 on the double coset $K\alpha K$ and 0 elsewhere. All elements of $\mathcal{H}(K\backslash GL_n(F)/K)$ are finite $\mathbb{C}$-linear sums of such functions. How does $1_{K\alpha K}$ act on V? Let

$$K\alpha K = \coprod_{i=1}^{m} \alpha_i K.$$

Then given $v \in V^K$

$$1_{K\alpha K}(v) := \int_{Gl_n(F)} 1_{K\alpha K}(g)vdg = \sum_{i=1}^{m} \alpha_i(v).$$

This extends linearly to all of $\mathcal{H}(K\backslash GL_n(F)/K)$. Passing to the direct limit the observe that there is a natural action of $\mathcal{H}(GL_n(F))$ on all of V by smoothness. Also observe that given $v \in V^K$, $e_K(v) = v$. Hence $\mathcal{H}(GL_n(F)) \cdot V = V$. If M is any $\mathcal{H}(GL_n(F))$-module we say it is non-degenerate if $\mathcal{H}(GL_n(F)) \cdot M = M$. The importance of this shift in perspective is the following fundamental result.

Theorem. *Let $K \subset GL_n(F)$ be an open compact subgroup. Let $\mathcal{A}_n(F)^K \subset \mathcal{A}_n(F)$ denote the subcategory such that the K-invariants are non-trivial. The functor from $\mathcal{A}_n(F)^K$ to the category of non-trivial irreducible finite dimension $\mathcal{H}(K\backslash GL_n(F)/K)$-modules given by $V \to V^K$ is an equivalence of categories.*

Remarks.

1. *This theorem can be expressed in terms of $\mathcal{H}(GL_n(F))$ if we add an extra admissibility condition on our non-degenerate $\mathcal{H}(GL_n(F))$-modules.*
2. *We can also relax irreducibility on both sides as long as we restrict to finite length representation.*
3. *The power of this theorem is that it allows us to study potentially infinite dimensional representations of $GL_n(F)$ using finite dimensional representation theory of some Hecke Algebra. The difficulty with this approach is that for arbitrary K, $\mathcal{H}(K\backslash GL_n(F)/K)$ may be very complicated.*

Spherical Representations

Let us restrict to a very special subcategory of $\mathcal{A}_n(F)$.

Definition. *Let $(\Pi, V) \in \mathcal{A}_n(F)$. We say that (Π, V) is spherical if $V^{GL_n(\mathcal{O}_F)} \neq \{0\}$.*

By the above we know that there is an equivalence of categories between spherical representations of $GL_n(F)$ and non-trivial finite dimensional $\mathcal{H}(GL_n(\mathcal{O}_F)\backslash GL_n(F)/GL_n(\mathcal{O}_F))$. We call this latter algebra the *spherical* Hecke algebra.

It is an important fact that $\mathcal{H}(GL_n(\mathcal{O}_F)\backslash GL_n(F)/GL_n(\mathcal{O}_F))$ is commutative. In fact

$$\mathcal{H}(GL_n(\mathcal{O}_F)\backslash GL_n(F)/GL_n(\mathcal{O}_F)) \cong \mathbb{C}[x_1^{\pm}, \cdots, x_n^{\pm}]^{S_n},$$

Where S_n is the symmetric group acting on $\{x_1, \cdots, x_n\}$ in the natural way. Because the non-trivial irreducible representations of a commutative algebra are 1-dimensional we deduce that given a spherical representation, $(\Pi, V) \in \mathcal{A}_n(F)$, then $dim_{\mathbb{C}} V^{GL_n(\mathcal{O}_F)} = 1$.

Remarks. *This structure theorem for $\mathcal{H}(GL_n(\mathcal{O}_F)\backslash GL_n(F)/GL_n(\mathcal{O}_F))$ is a special application of the Satake isomorphism. The Satake isomorphism in general gives a structure theorem for spherical Hecke algebras of arbitrary connected reductive groups, a concept we have not defined.*

Hence an isomorphism class of spherical representations of $GL_n(F)$ is given by a character of $\mathbb{C}[x_1^{\pm}, \cdots, x_n^{\pm}]^{S_n}$. But this is just the same as a semi-simple (contains a diagonal matrix) conjugacy class of $GL_n(\mathbb{C})$.

Recall that up to isomorphism unramified n-dimensional Φ-semisimple Weil-Deligne representations over $\mathbb{C}$ stand in one to one correspondence with semisimple conjugacy classes of $GL_n(\mathbb{C}$. Thus we deduce:

The Unramified Local langlands Correspondence for GL_n over F. *There is a natural bijection between the two sets:*

$$\{ \textit{ Isomorphism classes of unramified } n\textit{-dimensional } \Phi\textit{-semisimple Weil-Deligne representations of } W_F \textit{ over } \mathbb{C} \}$$

$$\updownarrow$$

$$\{ \textit{ Isomorphism classes of spherical irreducible smooth admissible representations of } GL_n(F) \textit{ on a complex vector space} \}$$

Proof. Both sets stand in natural bijection with semisimple conjugacy classes of $GL_n(\mathbb{C})$. □

Remarks. *This by far the easiest case of the correspondence. Somehow what is going on is that in the spherical case everything is collapsing to Abelian data - on the Weil-Deligne side an unramified representation σ is the direct sum of n characters of W_F. Hence by Local Class Field theory, σ gives n characters of $GL_1(F)$. We may package these together to form a character of $B(F) \subset GL_n(F)$, the subgroup of upper triangular matrices. This subgroup is generally called the standard Borel. The Spherical representation attached to σ is one which occurs as a subquotient of the induced representation to $GL_n(F)$. This principle will for the backbone of the Bernstein-Zelevinsky classification.*

Number Theory

Alexander Paulin

February 16, 2010

Lecture 18

Let $F/\mathbb{Q}_p$ be a finite extension and $n \in \mathbb{N}$. We have been studying irreducible smooth admissible complex representations of $GL_n(F)$. We denoted the set of isomorphism classes of such representations by $\mathcal{A}_n(F)$. Last time we singles out a particularly simple subset, the spherical representations. Recall that $(\Pi, V) \in \mathcal{A}_n(F)$ is spherical if $V^{GL_n(\mathcal{O}_F)} \neq \{0\}$. It turned out that $dim_{\mathbb{C}}(V^{GL_n(\mathcal{O}_F)}) = 1$. This was because the spherical Hecke algebra was commutative. It also turned out that such isomorphism classes stood in natural bijection with semisimple conjugacy classes of $GL_n(\mathbb{C})$. Today and next time we'll try to understand the Berstein-Zelevinsky classification of smooth irreducible admissible representations of $GL_n(F)$.

Parabolic Induction

Let $\underline{n} = (n_1, \cdots, n_r)$ be a partition of n. Let us write $G_{\underline{n}}(F)$ for the group

$$GL_{n_1}(F) \times \cdots \times GL_{n_r}(F).$$

Denote by $P_{\underline{n}}(F) \subset GL_n(F)$ the subgroup of matrices

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & * \\ & & \cdots & \\ & 0 & & \cdots \\ & & & A_r \end{pmatrix}$$

for $A_i \in GL_{n_i}$. We call $P_{\underline{n}}(F)$ the standard parabolic subgroup for the partition $\underline{\mathrm{n}}$. The subgroup $U_{\underline{n}}(F) \subset P_{\underline{n}}(F)$ consisting of matrices of form

$$\begin{pmatrix} I_{n_1} & & & \\ & I_{n_2} & & * \\ & & \cdots & \\ & 0 & & \cdots \\ & & & I_{n_r} \end{pmatrix}$$

where $I_{n_i} \in GL_{n_i}(F)$ is the identity matrix, is called the unipotent radical of $P_{\underline{n}}(F)$. Observe that we may embed $G_{\underline{n}}(F)$ in $P_{\underline{n}}(F)$ as matrices of the form:

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & 0 \\ & & \cdots & \\ & 0 & & \cdots \\ & & & A_r \end{pmatrix}$$

$G_{\underline{n}}(F)$ is called the Levi subgroup of $P_{\underline{n}}(F)$. If you have any familiarity with algebraic groups this is the usual deconstruction of a parabolic subgroup. In particular $GL_n(F)/P_{\underline{n}}(F)$ is compact.

Observe that every element $p \in P_{\underline{n}}(F)$ can be written uniquely in the form $p = mu$, where $m \in G_{\underline{n}}(F)$ and $u \in U_{\underline{n}}(F)$. This makes $P_{\underline{n}}(F)$ the semidirect product of $G_{\underline{n}}(F)$ and $U_{\underline{n}}(F)$. Consequently there is a natural projection homomorphism $P_{\underline{n}}(F) \to G_{\underline{n}}(F)$. If $\underline{n} = (1, \cdots, 1)$ then $P_{\underline{n}}(F)$ is called the standard Borel subgroup of $GL_n(F)$.

Let (Π_i, V_i) be an admissible complex representation of $GL_{n_i}(F)$ for each $i \in \{1, \cdots, r\}$. Then $\Pi_1 \otimes \cdots \otimes \Pi_r$ is a smooth admissible representation of $G_{\underline{n}}(F)$ on $V_i \otimes \cdots \otimes V_r$.. Using the projection of $P_{\underline{n}}(F)$ onto $G_{\underline{n}}(F)$, $\Pi_1 \otimes \cdots \otimes \Pi_r$ becomes an admissible representation on $P_{\underline{n}}(F)$.

Detour on Haar Measure

Observe that $P_{\underline{n}}(F)$ is a locally compact topological group. Hence it has a unique (up to scale) left Haar measure. If μ is a fixed left Haar measure of $P_{\underline{n}}(F)$ then for any $t \in P_{\underline{n}}(F)$, if $A \subset P_{\underline{n}}(F)$ is a Borel measurable subset then

$$A \to \mu(At^{-1}),$$

defines a new left Haar measure. Because left Haar measure is unique up to scale we know that there exists Δ, a character of $P_{\underline{n}}(F)$ taking values in the positive reals such that

$$\mu(At^{-1}) = \Delta(t)\mu(A).$$

Δ is called the modulus character of $P_{\underline{n}}(F)$. It essentially measure how far from being unimodular $P_{\underline{n}}(F)$ is. For example, if $P_{\underline{n}}(F)$ is unimodular then Δ is trivial.

Let $\Delta^{1/2}$ be the character of of $P_{\underline{n}}(F)$ taking in positive square root of Δ. For $\Pi_1 \otimes \cdots \otimes \Pi_r$ as

above we define the normalised smooth Parabolic induction of $\Pi_1 \otimes \cdots \otimes \Pi_r$ to representation of $GL_n(F)$ whose underlying vector space is

$$V = \{f : GL_n(F) \to V_i \otimes \cdots \otimes V_r | f \text{ smooth}, f(pg) = \Delta^{1/2}(p)(\Pi_1 \otimes \cdots \otimes \Pi_r)(p)f(g), \\ \text{for all } p \in P_{\underline{n}}(F), g \in G_{\underline{n}}(F)\}.$$

Here smooth means that it is is locally constant as a function on $GL_n(F)$. The action of $GL_n(F)$ on V is given by right translation. i.e. $g(f)(h) = f(hg)$. This gives a left action of $GL_n(F)$ on V which is smooth and admissible. The admissibility is because of the compactness of $GL_n(F)/P_{\underline{n}}(F)$. Even if the (Π_i, V_i) are irreducible this certainly does not means that V will be irreducible. Let us denote this representation by $\Pi_1 \times \cdots \times \Pi_r$.

A point of confusion is why have we introduced the modulus function? The reason is that if each of the (Π_i, V_i) are unitary, i.e. admit a Hilbert space structure whose inner product is invariant under the action of $GL_{n_i}(F)$ then the normalised smooth induction V is also unitary. If we omitted the modulus character then this would fail to be true. Unitary representations of topological groups are the main object of study within Harmonic Analysis.

Definition. *Given two complex representations of a group G, (π, V) and (μ, W), we say that (π, V) is isomorphic to a subquotient of (μ, W) if there are two G-stable subspaces $W_2 \subset W_1 \subset W$, such that the natural representation $(\mu, W_1/W_2)$ is isomorphic to (π, V). Note that if (μ, W) is semistable then all subquotients are subrepresentations. In general this is not the case.*

Definition. *An irreducible smooth admissible complex representation (Π, V) of $GL_n(F)$ is called supercuspidal if there exists no proper partition $\underline{n}$ such that Π is isomorphic to a representation of the form $\Pi_1 \times \cdots \times \Pi_r$, where each Π_i is an admissible complex representation of $GL_{n_i}(F)$. We denote by $\mathcal{A}_n(F)^0 \subset \mathcal{A}_n(F)$ the subset of isomorphism classes of supercuspidal representations of $GL_n(F)$.*

The importance of supercuspidal representations is shown by the following fundamental theorem of Bernstein and Zelevinsky:

Theorem. *Let Π be an irreducible smooth admissible representation of $GL_n(F)$. There exists a unique partition of $n = n_1 + \cdots + n_r$ and unique (up to isomorphism and ordering) supercuspidal representation Π_i of $GL_{n_i}(F)$ such that Π is a subquotient of $\Pi_1 \times \cdots \times \Pi_r$.*

We call the collection $(\Pi_1, \cdots, \Pi_r)$ the *supersuspidal support* of Π.

Powerful as this theorem is it still doesn't give us a good classification in turns of supercuspidal representation. By this I mean that two non-isomorphic smooth admissible irreducible representations of $GL_n(F)$ can have the same supercuspidal support. We need to refine the theorem. we'll do this next time.

Number Theory

Alexander Paulin

November 24, 2009

Lecture 19

Let $F/\mathbb{Q}_p$ be a finite extension. In order to try and understand the Local Lanlgands correspondence for $GL_{n/F}$ we have been trying to classify the isomorphism classes of smooth admissible irreducible complex representations of $GL_n(F)$. To do this introduced the important concept of parabolic induction. Recall that a supercuspidal representation is one that does not appear (up to isomorphism) as a subquotient of a proper parabolic induction. We denote the set of isomorphism classes of supercuspidal representations of $GL_n(F)$ by $\mathcal{A}_n^0(F)$. The following theorem tells us that the supercuspidals are the "building blocks" of smooth admissible irreducible representations of $GL_n(F)$:

Theorem. *Let Π be an irreducible smooth admissible representation of $GL_n(F)$. There exists a unique partition of $n = n_1 + \cdots + n_r$ and unique (up to isomorphism and ordering) supercuspidal representation Π_i of $GL_{n_i}(F)$ such that Π is a subquotient of $\Pi_1 \times \cdots \times \Pi_r$.*

Recall that the set $\{\Pi_1, \cdots, \Pi_r\}$ are called the supercusidal support of Π. A point of confusion is that it appears at first sight that the induced representation depends on the ordering of the partition. This is indeed true. However, the irreducible subquotients (up to isomorphism) are invariant.

It is also true that given a partition $n = n_1 + \cdots + n_r$ and a supercuspidal representation, Π_i, of $GL_{n_i}(F)$ for each i, then $\Pi_1 \times \cdots \times \Pi_r$ has finite length. This means that (up to isomorphism) there are only finitely many subquotients of $\Pi_1 \times \cdots \times \Pi_r$. Hence (up to isomorphism) there are only finitely many smooth admissible irreducible representations with the same supercuspidal support. We want to get a more refined classification than this.

There is a natural complex character on $GL_n(F)$ given by the composition of the determinant with the absolute value:

$$\begin{aligned} |det| : Gl_n(F) &\longrightarrow \mathbb{C}^* \\ g &\longrightarrow |det(g)| \end{aligned}$$

For any $s \in \mathbb{C}$ we get the character $|det|^s$. Given Π, a smooth admissible representation of $GL_n(F)$ we may *twist* Π with the character $|det|^s$ i.e. the representsation $g \to |det(g)|^s \Pi(g)$. We denote this new representation by $\Pi(s)$.

If Π is supercuspidal then $\Pi(s)$ is also supercuspidal. Define a partial order on $\mathcal{A}_n^0(F)$ by $\Pi \leq \Pi'$ if and only if there exists an integer $n \geq 0$ such that $\Pi' = \Pi(n)$. Hence ever finite interval Δ is of the form

$$\Delta(\Pi, m) = [\Pi, \Pi(1), \cdots, \Pi(m-1)].$$

The integer m is called the length of the interval and nm is called the degree. We write $\Pi(\Delta)$ for the representation $\Pi \times \cdots \times \Pi(m-1)$ of $GL_{nm}(F)$.

Two finite intervals Δ_1 and Δ_2 are said to be linked if neither contains the other and $\Delta_1 \cup \Delta_2$ is a finite interval. We say that Δ_1 *precedes* Δ_2 if they are linked and the minimal element of Δ_1 is smaller that the minimal element of Δ_2. We are now in a position to state the Bernstein-Zelevinsky classification.

Theorem. *1. For any finite interval $\Delta \subset \mathcal{A}_n^0(F)$, $\Pi(\Delta)$ has a unique irreducible smooth admissible quotient $Q(\Delta)$.*

2. Let $\Delta_1 \subset \mathcal{A}_{n_1}^0(F), \cdots, \Delta_r \subset \mathcal{A}_{n_r}^0(F)$ be finite intervals such that for $i < j$, Δ_i does not precede Δ_j (this is the empty condition is $n_i \neq n_j$). Then the representation $Q(\Delta_1) \times \cdots \times Q(\Delta_r)$ admits a unique irreducible quotient $Q(\Delta_1, \cdots, \Delta_r)$.

3. Let Π be a smooth admissible irreducible complex representation of $GL_n(F)$. Then it is isomorphic to a representation of form $Q(\Delta_1, \cdots, \Delta_r)$ for a unique (up to permutation) collection of intervals $\Delta_1, \cdots, \Delta_r$ such that Δ_i does not precede Δ_j for $i < j$.

4. Under the hypothesis of (ii), the representation $Q(\Delta_1) \times \cdots \times Q(\Delta_r)$ is irreducible if and only if no two intervals Δ_i and Δ_j are linked.

Lets do the special case where $n = 2$. This is easier as there is only one non-trivial standard parabolic, the standard borel (upper triangular matrices). The levi component of the standard borel is just the subgroup of diagonal matrices (a maximal torus). Hence the blocks in the levi component are just $GL_1(F)$. Thus if Π is a smooth admissible representation of $GL_2(F)$ which is not supercuspidal then it must be induced from two smooth characters of $GL_1(F)$.

More precisely, if χ_1, χ_2 are two smooth complex characters of $GL_1(F)$, then we may form the normalised parabolic induction, $\mathcal{B}(\chi_1, \chi_2)$. By the classification we know that if $\chi_1/\chi_2 \neq |det|^{\pm 1}$ (i.e. they are not linked) then $\mathcal{B}(\chi_1, \chi_2)$ is irreducible. In this case we write $\mathcal{P}(\chi_1, \chi_2) = \mathcal{B}(\chi_1, \chi_2)$.

Such representations are called *Principal Series*. The infinite dimensional spherical smooth admissible irreducible complex representations of $GL_2(F)$ are isomorphic to a principal series representation where both character are trivial on $\mathcal{O}_F^*$.

The other case is when χ_1 and χ_2 are linked, i.e. $\chi_1/\chi_2 \neq |det|^{\pm 1}$. There are two possible things that can happen in this situation. If $\chi_2 = \chi_1|det|$ then χ_1 precedes χ_2 in the above terminology. Hence the classification only works if they are in the same interval. In this case $\mathcal{B}(\chi_1, \chi_2)$ is reducible, of length two. We denote the unique irreducible quotient by $Sp(\chi_1)$. Such representations are called *Special*. They are also infinite dimensional. If χ_1 is trivial then it is called the Steinberg representation.

The final case to consider is when $\chi_1 = \chi_2|det|$, i.e. when χ_2 precedes χ_1. For the classification to work in this case we must think about χ_1 and χ_2 as distinct intervals. In this case the the irreducible quotient is just the character $|det|^{1/2}\chi_1(det)$. This together with the supercuspidals exhausts all the smooth admissible irreducible representations of $GL_2(F)$.

Let's return to the Local Langlands correspondence. Recall that we are trying to find a bijection between isomorphism classes of smooth admissible irreducible complex representations of $GL_n(F)$ and isomorphism classes of complex n-dimensional Φ-semisimple Weil-Deligne of W_F. Recall that we showed that any such Weil-Deligne representation is the direct sum of ones of form $\rho' \otimes Sp(m)$, where ρ' is a an irreducible complex representation of the W_F (N=0) and $Sp(m)$ is given by

$$V = \mathbb{C}e_0 + \mathbb{C}e_1 + \cdots + \mathbb{C}e_{m-1}$$

$$\rho_0(\sigma)e_i = ||\sigma||^i e_i \ \forall \sigma \in W_F, \ i \in \{0, 1, \cdots m-1\}$$

$$Ne_i = e_{i+1} \ \forall \ i \in \{0, 1, \cdots m-2\}; \ Ne_{m-1} = 0.$$

This together with the Berstein-Zelevinsky classification indicates that ρ' should correspond to a supercusidal Π' and $\rho' \otimes Sp(m)$ should correspond to the unique irreducible quotient given by $Q(\Delta)$, where $\Delta = [\Pi', \cdots \Pi'(m-1)]$. If (ρ, N) is the direct sum of $(\rho'_i \otimes Sp(m_i))$ (corresponding to $Q(\Delta_i)$ for $\Delta_i = [\Pi'_i, \cdots, \Pi'_i(m_i - 1)]$) then it should correspond to the representation $Q(\Delta_1, \cdots, \Delta_r)$, making sure to order the intervals in accordance with the classification.

Thus the Bernstein- Zelevinsky classification reduces proving the Local Langlands correspondence for $GL_n(F)$ to finding a natural bijection between $\mathcal{A}_n^0(F)$ and complex n-dimensional irreducible representations of W_F. Of course the operative word is natural, something we have not made precise. To do this would take us too far afield. It was finally settled by Harris and Taylor in 2000 using very sophisticated geometric techniques. If you are feeling brave have a look at their book: "the Cohomology of some Simple Shimura Varieties".

That's about all the local stuff I want to talk about. Next time: Global Langlands!

Number Theory

Alexander Paulin

December 1, 2009

Lecture 20

Thus far we have been considering the generalisation of local class field theory to higher dimensions. Let us now turn to the global picture.

Recall that we were able to reformulate global class field theory in the language of Hecke characters. Let F be a number field. Fix an algebraic closure $\bar{F}$. For every place v fix an algebraic closure $\bar{F}_v$ and an embedding $\bar{F} \subset \bar{F}_v$. Recall that this fixes embeddings $G_{F_v} \subset G_F$. Recall the fundamental definition:

Definition. *A Hecke character of F is a continuous homomorphism (for the usual topology on $\mathbb{C}$)*

$$GL_1(F)\backslash GL_1(\mathbb{A}_F) \longrightarrow \mathbb{C}^*.$$

Recall that a finite order Hecke character was one whose image was finite. Global class field theory established a natural bijection:

$$\{ \text{ Hecke characters of } F \text{ of finite order } \}$$

$$\updownarrow$$

$$\{ \text{ One dimensional continous complex representations of } G_F \}$$

We were able to push this slightly further by introducing the concept of an arithmetic Hecke characker. Recall these where Hecke character whose restiction to the infinite component of $GL_1(\mathbb{A}_F)$ was inherently algebraic. For $F = \mathbb{Q}$, χ is arithmetic if and only if $\chi|_{\mathbb{R}_{>0}} = |.|^k$ for some $k \in \mathbb{Z}$. We also saw that these corresponded to Galois theoretic data.

Let p be a prime number. Fix an algebraic closure $\bar{\mathbb{Q}}_p$. A p-adic character of G_F is a continuous (for the p-adic topology on $\bar{\mathbb{Q}}_p$) homomorphism:

$$\rho : G_F \to GL_1(\bar{\mathbb{Q}}_p).$$

By the Baire category theorem the image is actually contained in $GL_1(E)$ for some finite extension $E/\mathbb{Q}_p$. We singled out a special class of such representations which we called *potentially semistable*. In general we did not make this notion precise but for $F = \mathbb{Q}$ it meant that ρ was a product of a finite order character and an integer power of the p-adic cyclotomic character. This allowed us to expand the above bijection:

$$\{ \text{ Arithmetic Hecke Characters of } F \ \}$$

$$\updownarrow$$

$$\{ \text{ One dimensional } p\text{-adic potentially semi-stable representations of } G_F \ \}$$

Now we are in a position to consider what the appropriate generalisations of this may be to higher higher dimensions.

1 The Global Langlands Philosophy

This whole last section is an order of magnitude deeper than what has been done thus far. I'll do my best to outline what the landscape looks like.

Perhaps the easiest issue to address first is what the correct analogue of a one dimensional p-adic potentially semi-stable representation should be. It would take too long to properly address this question but I'll give you an outline.

An n-dimensional p-adic representation of G_F is a continuous (for the p-adic topology on $\bar{\mathbb{Q}}_p$) homomorphism:

$$\rho : G_F \to GL_n(\bar{\mathbb{Q}}_p).$$

Again by the Baire category theorem we could assume that the image is in $GL_n(E)$ for some finite extension $E/\mathbb{Q}_p$. If ρ has finite image then in fact we can assume that E is a finite extension on $\mathbb{Q}$. Thus continuous n-dimensional complex representations (which are always finite order) can naturally consider as examples of p-adic representations.

Notice that in the one dimensional case the representations which were of interest had some restriction: they where potentially semi-stable. This condition is something to do with the restrictions $\rho|_{G_{F_v}}$ where $v|p$. Being potentially semistable in the higher dimensional case is much more complicated, but is still a condition to do with the restrictions $\rho|_{G_{F_v}}$ where $v|p$. The definiton was given by Jean-Marc Fontaine and involves something called p-adic Hodge theory.

Classical Hodge theory addresses the issue of how the deRham cohomology of a compact complex manifold decomposes. p-adic Hodge theory does something similar for smooth projective varieties defined over p-adic fields. This gives a hint that something geometric is going on.

1.1 Etale Cohomology

Let X be a smooth, projective variety over $Spec(F)$. Let $\bar{X}$ be the bases change to $Spec(\bar{F})$. Note that G_F acts on $\bar{X}$, i.e. given $\sigma \in G_F$ there is a natural morphism of schemes (not over $\bar{F}$)

$$\sigma : \bar{X} \to \bar{X}.$$

Fix a prime p and $d \in \mathbb{N}$. Let $\underline{\mathbb{Z}/p^d\mathbb{Z}}$ denote the etale constant sheaf on $\bar{X}$ associated to the abelian group $\mathbb{Z}/p^d\mathbb{Z}$. The etale bit means that we are putting the "etale topology" on $\bar{X}$ instead of the usual Zariski topology. This is a conceptual jump. The etale "topology" is actually a "topology" on a category associated to $\bar{X}$, and not on $\bar{X}$ as a set of points. Anyway, taking the derived functors of the usual global sections functor into abelian groups gives the etale chomology groups:

$$H^i_{et}(\bar{X}, \underline{\mathbb{Z}/p^d\mathbb{Z}}), \quad i \in \mathbb{N} \cup \{0\}.$$

Note that by functoriality on the coefficients we have a natural projective limits:

$$H^i_{et}(\bar{X}, \mathbb{Z}_p) := \varprojlim_d H^i_{et}(\bar{X}, \underline{\mathbb{Z}/p^d\mathbb{Z}}).$$

Note that by functoriality on the coefficients $H^i_{et}(\bar{X}, \mathbb{Z}_p)$ is naturally a $\mathbb{Z}_p$-module. We define the p-adic (often in the literature they say l-adic, but we've fixed different conventions) cohomology groups of $\bar{X}$ to be

$$H^i_{et}(\bar{X}, \mathbb{Q}_p) := H^i_{et}(\bar{X}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Finally we write

$$H^i_{et}(\bar{X}, \bar{\mathbb{Q}}_p) := H^i_{et}(\bar{X}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \bar{\mathbb{Q}}_p.$$

Fact: $H^i_{et}(\bar{X}, \bar{\mathbb{Q}}_p)$ is a finite dimensional $\bar{\mathbb{Q}}_p$-vector space equipped with a natural continuous $\bar{\mathbb{Q}}_p$-linear action of G_F.

This means that the p-adic cohomology groups of smooth projective varieties over F give a natural source of p-adic representations of G_F!.

Theorem. *As a G_F representation $H^i_{et}(\bar{X}, \bar{\mathbb{Q}}_p)$ is potentially semistable.*

The geometric behaviour of X is intimately connect to the properties of $H^i_{et}(\bar{X}, \bar{\mathbb{Q}}_p)$ as a representation of G_F.

Definition. *Let v be a finite place of F. Let X_v be the base change of X to F_v. It is still smooth and projective. We say that X has good reduction at v is there exists a scheme $\mathfrak{X}$*

together with a smooth projective morphism

$$\begin{array}{c} \mathfrak{X} \\ \downarrow \\ Spec(\mathcal{O}_{F_v}) \end{array}$$

Such that there is a cartesian (fiber product) diagram

$$\begin{array}{ccc} X_v & \longrightarrow & \mathfrak{X} \\ \downarrow & & \downarrow \\ Spec(F_v) & \longrightarrow & Spec(\mathcal{O}_{F_v}) \end{array}$$

Facts:

1. For all but finitely many finite places of F, X has good reduction.
2. If X has good reduction at v and v does not divide p then the G_F-representation $H^i_{et}(\bar{X}, \bar{\mathbb{Q}}_p)$ is unramified at v. This means that the restriction to the interia subgroup of G_{F_v} is trivial.

Definition. *We say that a p-adic representation of G_F is geometric is it is isomorphic to a subquotient of a p-adic representation coming from the p-adic cohomology of a smooth projective variety over F. We come to the following profound conjecture:*

The Fontaine-Mazur Conjecture. *Let ρ be a p-adic representation of G_F. Then ρ is geometric if an only if it is potentially semi-stable and is unramified at all but finitely many places not dividing p.*

If you want to believe the Fontaine-Mazur conjecture then you could pretty much take this as the definition for being potentially semi-stable. For 2-dimensional representations this has almost been settled by work of many people.

There is an asymmetry in this picture: p was chosen arbitrarily. To X we have a collection of representations for every prime p. We also saw this with the one dimensional case. Unsurprisingly there is strong compatibility between these different representations: They form something called a compatible system. If we have time I'll make this precise next time.

The upshot of all this is that we have a candidate for the Galois theoretic side of the "Global Langlands Correspondence".

Number Theory

Alexander Paulin

December 3, 2009

Lecture 21

Let F be a number field. Fix an algebraic closure $\bar{F}$. For every place v fix an algebraic closure $\bar{F}_v$ and an embedding $\bar{F} \subset \bar{F}_v$. Recall that this fixes embeddings $G_{F_v} \subset G_F$.

Let X be a smooth projective variety over F and p a fixed prime number. Recall that we were able to canonically associate to X, via a construction in etale cohomology the finite dimensional $\bar{\mathbb{Q}}_p$-vector spaces :$H^i_{et}(\bar{X}, \bar{\mathbb{Q}}_p)$. By functoriality of cohomology these vector spaces naturally came equipped with continuous $\bar{\mathbb{Q}}_p$-linear actions of G_F. A p-adic representation of G_F was said to be *geometric* if it was isomorphic to a subquotient of such a representation. The Galois theoretic side of the a higher dimensional global class field theory should then be the set:

$$\{ \text{ Isomorphism classes of } \textit{geometric } p\text{-adic representations of } G_F. \}$$

As a geometer it is natural to ask whether the a *geometric* p-adic representation of G_F corresponds to something truly geometric. Grothendieck introduced the concept of a *pure motive* to try and do this. The idea is that the cohomology groups of X can decompose (as vector spaces) , without X decomposing as a variety. Grothendieck suggested that this decomposition did have geometric meaning once one enlarged the category of smooth projective varieties over F to what he called the category of pure motives over F, denoted $\mathcal{M}$. This idea is still fuzzy - many natural questions are still unresolved. What is true is that $\mathcal{M}$ is Abelian and semi-simple and to every pure motive we may canonically associate a *geometric* p-adic representation of G_F. The category of pure motives over F isn't so hard to define. What's hard is proving it has reasonable properties - the standard conjectures (unproven after 40 years) imply that the process of associating a *geometric* p-adic representation to a pure motive is functorial. If we want to be really fancy we could say that the Galois theoretic side of the a higher dimensional global class field theory should then be:

$$\{ \text{ Grothendieck's category of pure motives over } F. \}$$

Automorphic representations of $GL_{n/F}$

What is the higher dimensional generalisation of a Hecke character over F. This is a hard question. Firstly observe that Hecke characters are inherently real analytic objects. They are certain continuous one dimensional complex representations of $GL_1(\mathbb{A}_F)$. The *certain* means that they are trivial on $GL_1(F) \subset GL_n(\mathbb{A}_F)$. The local case would suggest that what we want is some kind of big infinite dimensional complex representation of $GL_n(\mathbb{A}_F)$. This is indeed the case. It also has to have some kind of invariance properties under $GL_n(F) \subset GL_n(\mathbb{A}_F)$. Finally it has to be fundamentally real analytic. The correct concept is that of an *automorphic representation* of $GL_n(\mathbb{A}_F)$.

Let χ be a unitary Hecke character, i.e. $|\chi(g)| = 1$ for all $g \in GL_1(F)\backslash GL_1(\mathbb{A}_F)$. Let $Z(\mathbb{A}_F) \subset GL_n(\mathbb{A}_F)$ denote the center. There is a natural identification $GL_1(\mathbb{A}_F) = Z(\mathbb{A}_F)$. Recall that $GL_n(\mathbb{A}_F)$ is a locally compact topological group. It is unimodular and comes equipped with a a unique (up to scale) left and right Haar measure. This descends to a Haar measure on the quotient $GL_n(F)\backslash GL_n(\mathbb{A}_F)$. This further descends to a Haar measure, which we denote dg, on the quotient $Z(\mathbb{A}_F)GL_n(F)\backslash GL_n(\mathbb{A}_F)$.

Definition. *The space of L^2-automorphic forms with central character χ is the complex vector space*

$$L^2(GL_n(F)\backslash GL_n(\mathbb{A}_F); \chi)$$

of all measurable $\varphi : GL_n(F)\backslash GL_n(\mathbb{A}_F) \to \mathbb{C}$ such that $\varphi(zg) = \chi(z)\varphi(g)$ for all $z \in Z(\mathbb{A}_F)$ and

$$\int_{Z(\mathbb{A}_F)GL_n(F)\backslash GL_n(\mathbb{A}_F)} |\varphi(g)|^2 dg < \infty.$$

This is naturally a Hilbert space and the group $GL_n(\mathbb{A}_F)$ acts by right translation on this space preserving the norm; hence $L^2(GL_n(F)\backslash GL_n(\mathbb{A}_F); \chi)$ is a unitary representation of $GL_n(\mathbb{A}_F)$.

Definition. *An automorphic representation of $GL_n(\mathbb{A}_F)$ with central character χ is an irreducible (topologically) constituent of $L^2(GL_n(F)\backslash GL_n(\mathbb{A}_F); \chi)$.*

We should remark that irreducible constituent means those which occur discretely (are subrepresentations), and those which occur continuously (as a direct integral). This is difficult functional analyisis. Just think about it as a subrepresentation for the moment.

Let π be an automorphic representation of $GL_n(\mathbb{A}_F)$. Let r_1 be the number of real places of F and r_2 be the number of complex places of F. Then let

$$K_\infty = O(n)^{r_1} \times U(n)^{r_2} \subset GL_n(\prod_{v|\infty} F_v)$$

and

$$K_f := \prod_{v\ finite} GL_n(\mathcal{O}_{F_v}).$$

Then

$$K = K_f \times K_\infty \subset GL_n(\mathbb{A}_F),$$

is a maximal compact subgroup.

We say that $v \in \pi$ is K-finite if $\mathbb{C}[K]v \subset \pi$ is finite dimensional. We denote the space of K-finite vectors by $\pi_K \subset \pi$. It is a fact that π_K is dense in π. Unfortunately π_K is not closed under the action of $GL_n(\mathbb{A}_F)$. The K_∞-finiteness is not preserved under the action of $GL_n(\prod_{v|\infty} F_v)$. However, π_K is preserved under the action of $GL_n(\mathcal{A}_F^\infty)$. In this way π_K is a smooth, admissible complex irreducible representation of $GL_n(\mathcal{A}_F^\infty)$. These definitions are the same as in the local case.

For every finite place v let V_v be a complex, smooth, admissible, irreducible representation of $GL_n(F_v)$. Furthermore assume that for all but finitely many places V_v is spherical (i.e. has a unique (up to scale) $GL_n(\mathcal{O}_{F_v})$-fixed vector u_v. We define the restricted tensor product by

$$V = \otimes_v' V_v = \varinjlim_S ((\otimes_{v \in S} V_v) \otimes (\otimes_{v \notin S} u_v)).$$

Where S runs over all finite subset of the finite places of F containing those places for which V_v is not spherical. It is a fact that V is a smooth, admissible, irreducible complex representations.

Theorem. *Let π be an automorphic representation of $GL_n(\mathbb{A}_F)$. Then as a $GL_n(\mathcal{A}_F^\infty)$-representation π_K decomposes uniquely (up to isomorphism) into the restricted tensor product:*

$$\pi_K = \otimes_v' \pi_v,$$

where π_v is a smooth, admissible, irreducible, complex representation of $GL_($F_v$)$, spherical for almost all v.

Let S_π denote the finite subset of the finite places of F such that π_v is not spherical. Recall that by the Satake isomorphism any spherical representation π_v of $GL_n(F_v)$ is determined up to isomorphism by a semi-simple conjugacy class of $GL_n(\mathbb{C})$. Hence to any automorphic representation of $GL_n(\mathbb{A}_F)$ we may associate the data

$$(\Phi_v)_{v \notin S_\pi},\ \Phi_v \subset GL_n(\mathbb{C}),$$

where Φ_v is a semisimple conjugacy class.

The Global Langlands Correspondence

We are finally in a position to state probably the fundamental conjecture in number theory.

Let ρ be an n-dimensional, p-adic representation of G_F such thast ρ is unramified (away

from p) at almost all finite places of F. Let S_ρ be the finite subset of the finite places of F for which ρ is ramified. Let v be a place not dividin P. We may restrict the representation to give

$$\rho|_{G_{F_v}} : G_{F_v} \to GL_n(\bar{\mathbb{Q}}_p).$$

By Grothendieck's abstract monodromy theorem we may associate to this data an n-dimensional Φ-semisimple Weil-Deligne representation of W_F. Hence for $v \notin S_\rho$ we have an associate *unramified* Weil-Deligne representation. We have seen that such a representation corresponds to a semi-simple conjugacy class $\Upsilon_v \subset GL_n(\mathbb{C})$

Recall that if ρ is geometric then it satisfies the above property (smooth projective varieties over F have good reduction almost everywhere). Hence to any ρ, a geometric, p-adic representation of G_F we may canonically associate the data:

$$(\Upsilon_v)_{v \notin S_\rho},\ \Upsilon_v \subset GL_n(\mathbb{C}).$$

Definition. *We say that ρ, an n-dimensional, p-adic representation of G_F, is automorphic if*

1. *ρ is unramified away from a finite set of places S_ρ.*
2. *There exist π, an automorphic representation of $GL_n(\mathbb{A}_F)$, such that there exists S, a finite set of places of F, contain both S_ρ and S_π such that*

$$(\Upsilon_v)_{v \notin S} = (\Phi_v)_{v \notin S}.$$

Global Langlands Reciprocity (Version 1). *Every geometric p-adic representation of G_F is automorphic.*

Recall that to any Grothendieck pure motive over F we can associate a geometric p-adic representation of G_F.

Definition. *A Grothendieck pure motive is automorphic if its associate p-adic representation is.*

Global Langlands Reciprocity (Version 2). *Every Grothendieck pure motive over F is automorphic*

This is about a deep as mathematics has made it thus far. We are a very very long way from proving this. Philosophically it ways that arithmetic and geometry fundamentally encode analytic data - a kind of grand unified theory of mathematics. To give you some idea of how hard it has to be. Let's do a special case:

Let E be an elliptic curve over $\mathbb{Q}$. Remember that this is a smooth projective variety over $spec(\mathbb{Q})$, so all the machinery of Grothendieck's etale cohomology may be applied to it. In particular $H^1_{et}(\bar{E}, \bar{\mathbb{Q}}_p)$ is a 2-dimensional p-adic representation of $G_{\mathbb{Q}}$. It corresponds to a Gorthendieck motive which we call $h^1(E)$. The Taniyama-Shimura conjecture (Wile's

Theorem) states that $h^1(E)$ is automorphic (or modular in other terminology). This means that there is an automorphic representation of $GL_2(\mathcal{A}_{\mathbb{Q}})$ to which it corresponds. Classical modular forms give such representations. In loose terminology, when people say that E is modular, they really mean that $h^1(E)$ is automorphic. From the perspective of the Global Langlands Reciprocity conjecture this is a very very special case. If a proof of Langlands reciprocity is the same as swimming the Atlantic, we're only a few miles in. How long will the swim take? Only time will tell.