Primitive Galois Representations

Zavosh Amir-Khosravi

December 29, 2005

Abstract

The first section is a survey of some standard results from algebraic number theory, specifically local fields. The second section pertains to Clifford's theorem in representation theory and some consequences. In the third section we will combine the first two to give a general result concerning irreducible galois representations.

1 Algebraic Number Theory

Definition 1.1. *A valuation $|.|$ on a field k is a map from k to the real numbers such that $\forall a, b \in k$:*

1. $|a| >= 0$ *with equality iff* $a = 0$
2. $|ab| = |a||b|$
3. $|a + b| <= |a| + |b|$

A valuation is called non-archimedean when it satisfies the following stronger *ultrametric* inequality:

$$|a + b| <= max\{|a|, |b|\}$$

Examples: The normal absolute value on the field $\mathbb{C}$ of complex numbers. The *p-adic valuation* on $\mathbb{Q}$ is non-archimedean.

For a field k endowed with a valuation let G_k denote the set of non-zero values a valuation takes. G_k is a multiplicative subgroup of the positive real numbers. A valuation is called *discrete* if this subgroup is discrete in the standard topology of the real line. The *p-adic* valuation on $\mathbb{Q}$ is a discrete valuation.

Given a discrete valuation field k, consider the set $\{a : |a| < 1\}$. There must be an element π such that $|\pi|$ is the supremum of $|.|$ over the set. Then we have:

Lemma 1.1. *Given π as above in a discrete valuation field k, $\forall a \in k, |a| = |\pi|^n$ for some $n \in \mathbb{Z}$.*

Proof. Suppose without loss of generality that $|\pi^{n+1}| < |a| < |\pi^n|$, then $|\pi| < |a/\pi^n| < 1$, a contradiction. □

This shows in particular that the valuation group of a discrete valuation field is cyclic.

Let k be a non-archimedean valuation field with valuation $|.|$. The set

$$\mathfrak{o} = \{x \in k : |x| <= 1\}$$

is clearly a ring, called the ring of *integers* .

The set

$$\mathfrak{p} = \{x \in k : |x| < 1\}$$

is also clearly a maximal ideal in $\mathfrak{o}$, called the *valuation ideal* . Hence the quotient $\mathfrak{o}/\mathfrak{p}$ is a field, called the *residue class field* of k.

The order of the residue class field is called the *residue characteristic* of k.

Example:

For $\mathbb{Q}_5$ we have:

$$\mathfrak{o} = \{\sum_{k=0}^{\infty} a_k 5^k : a_k \in \{0, ..., 4\}\}$$

$$\mathfrak{p} = \{x \in \mathfrak{o} : a_0 \neq 0\} = 5\mathfrak{o}$$

$$\mathfrak{o}/\mathfrak{p} \cong F_5$$

It is clear that the valuation defines a norm on the field k, and so induces a natural topology on it. Furthermore any valuation field can be made complete with respect to the valuation. An example is $\mathbb{Q}_p$, the completion of the rationals with respect to the *p-adic* valuation.

The following is an important result concerning extensions of complete valuation fields:

Theorem 1.1. *Let K be a finite extension of a complete valuation field k with valuation $|.|$. There is a unique extension of $|.|$ to K, and furthermore, K is complete with respect to this extension.*

Proof. We shall only prove the first half of the theorem here. For a proof of the completion, we refer to [Cassels, p117].

Consider K as a vector space over k. For $a \in K$ consider the linear map $x \mapsto ax$. By $N_{K/k}$ denote the determinant of this transformation. Clearly $N_{K/k}(a) \in k$. Furthermore, $N_{K/k}$ is multiplicative and if $a \in k$, then $N_{K/k}(a) = a^n$, where $n = [K : k]$. Let $|.|_K$ on K be defined by:

$$|a|_K = (|(N_{K/k}(a)|)^{1/n}$$

It follows that $|.|_K$ is an extension of $|.|$ to K. It is a standard theorem of analysis that any two norms on a vector space over a complete field are equivalent, hence any other extension of $|.|$ to K would be equivalent to $|.|_K$, but because they take the same values on k, they would have to be equal.

□

From now on we will assume that k is a complete discrete valuation field and that K is an extension of k. We denote the valuation ideals of k and K by $\mathfrak{o}_k$ and $\mathfrak{o}_K$ and similarly denote $\mathfrak{p}_k$ and $\mathfrak{p}_K$ to be the respective valuation ideals. It is clear from the definitions that $\mathfrak{o}_k \subset \mathfrak{o}_K$ and $\mathfrak{p}_k \subset \mathfrak{p}_K$. It follows then that the residue class field of k, $\mathfrak{o}_k/\mathfrak{p}_k$ embedds naturally in the residue class field $\mathfrak{o}_K/\mathfrak{o}_k$. We call the degree of this extension, i.e $[\mathfrak{o}_K/\mathfrak{p}_K : \mathfrak{o}_k/\mathfrak{p}_k]$, the *residue class degree* , denoted by $f(K/k)$.

Theorem 1.2. *For $k \subset K \subset L$ we have:*

$$f(L/k) = f(L/K)f(K/k)$$

Proof. This follows immediately from the definition and the multiplicative nature of extension degrees. □

For $k \subset K$, the valuation group G_k is a subgroup of G_K.

Definition 1.2. *The index $[G_K : G_k]$, denoted $e(K/k)$ is called the ramification index of K over k.*

We immediately have the following obvious result:

Theorem 1.3. *For $k \subset K \subset L$:*

$$e(L/k) = e(L/K)e(K/k)$$

Note that in a discrete valuation field, we have that G_k is cyclic, and by the definition of the norm over K, it follows that G_K/G_k is a subgroup of $\mathbb{Z}/n\mathbb{Z}$, and so $[G_K : G_k]|n$. The following more precise result is inseparable from the topic, but as we won't have need for it, we shall only state it without proof.

Theorem 1.4. *Suppose k is a complete discrete valuation field and K is an extension of k such that $[K : k] < \infty$. Then:*

$$e(K/k)f(K/k) = [K : k]$$

Now we can state the definitions required for the rest of this article.

Definition 1.3. *An extension L/K of discrete valuation fields is said to be* **non-ramified** *if $e(L/K) = 1$.*

Restricting ourselves to fields k of finite residue characteristic χ, we make the following definition.

Definition 1.4. *An extension K/k is said to be* **tamely ramified** *if χ does not divide $e(L/K)$.*

A field extension K/k that is not tamely ramified is said to be **wildly ramified** .

Examples:

Let K = $\mathbb{Q}_5(\sqrt{2})$ and $k = \mathbb{Q}_5$ with the valuation $|.|_5$. 2 is not a square in $\mathfrak{o}_k \cong F_5$, so $f(K/k) = 2$, and therefore $e(K/k) = 1$, i.e K/k is an unramified extension.

For K=$\mathbb{Q}_5(\sqrt{5})$ and $k = \mathbb{Q}_5$, K is a vector space over k with basis $\{1, \sqrt{5}\}$. G_k is generated by 1/5 and G_K is generated by $|\sqrt{5}|_5 = |det(\begin{smallmatrix}0 & 5\\ 1 & 0\end{smallmatrix})|_5^{1/2} = |5|_5^{1/2} = 1/\sqrt{5}$. Therefore $e(K/k) = 2$ and so this extension is tamely ramified. Alternately, 5 is a square in F_5 therefore $f(K/k) = 1$ so $e(K/k) = 2$.

Similarly one can check that $\mathbb{Q}_5(\sqrt[5]{5})$ is a wildly ramified extension over $\mathbb{Q}_5$.

It follows immediately from the definition of tame ramification that if L and K are two tamely ramified extensions of k contained in the separable algebraic closure $\bar{k}$ of k, then the subfield of $\bar{k}$ generated by both L and K is also tamely ramified over k.

The subfield of $\bar{k}$ generated by all tamely ramified extensions of k is called the **maximal tamely ramified extension** of k, denoted by K_{tr}. K_{tr} is a normal extension of k and so $Gal(\bar{k} : K_{tr})$ is a subgroup of the Galois group $G = Gal(\bar{k}/k)$, denoted by P_k, also called the **wild ramification subgroup** of G. This means that the quotient G/P_k is the Galois group of the (normal) extension K_{tr}/k.

Here inevitably we must state certain results from algebraic number theory without proof. The reader is referred to [Brighton] for a complete exposition, specifically the chapter on Local Fields written by A. Fröhlich.

It turns out that every extension of k is a tower of a non-ramified, tamely ramified, and a wildly ramified extension. For a complete discrete valuation field of residue characteristic p, every extension of K_{tr} has a p-power degree. Therefore the Galois group of the extension $\bar{k}/K_{tr}$ is the inverse limit of p-groups, i.e a pro p-group.

Now to state the next result from algebraic number theory we need an algebraic definition.

Definition 1.5. *A group G is said to be supersolvable if there exists a sequence of normal subgroups $H_0 \lhd H_1 \lhd \cdots \lhd H_n$ such that $H_0 = 0$ and $H_n = G$ where each H_{i+1}/H_i is cyclic.*

A number theoretic result states that $Gal(K_{tr}/k)$ is supersolvable. The associated normal subgroups are defined through the action of the Galois group and the valuation on K and are called the **ramification groups** .

The remaining parts of this survery paper are dedicated to studying the representations of G and their restriction to the subgroup P_k.

2 Clifford's Theorem

In this section we will state and prove a part of a standard result of Clifford's that we will use later. A second result of Clifford will also be stated without proof. The reader can refer to [Dornhoff, p140] for a complete statement and proof of both results.

Notation: For simplicity we will sometimes write gw instead of $\pi(g)w$.

Theorem 2.1. *Let (π, V) be an irreducible representation of G, and let N be a normal subgroup of G. Let W be a subspace of V invariant under the action of N such that $(\pi|_N, W)$ is an irreducible representation. Let $gW = \{gw : w \in W\}$ Then we have:*

(1) $V = \sum_{g\in G} gW$ and $(\pi|_N, V)$ is completely reducible.

(2) For $\alpha \in I$ Let W_α denote the representatives of equivalence classes of irreducible subrepresentations of N in the space V. Let V_α denote the direct sum of all representations equivalent to W_α. Then $V = \bigoplus_{\alpha\in I} V_\alpha$.

(3) G acts transitively on the set $\{V_\alpha\}$.

(4) If $H_\alpha = \{g \in G|gV_\alpha = V_\alpha\}$, then V_α is irreducible under the action of H_α and $V \cong Ind_H^G(V_\alpha) = kG \bigotimes_{kH_\alpha} V_\alpha$

Proof. Proof of (1): Let $gW = \pi(g)w : w \in W$. Consider $U = \sum_{g\in G} gW$. U is invariant under the action of G, but V is irreducible, hence necessarily $V = U = \sum_{g\in G} gW$. We have $(\pi|_N, gW)$ is a representation since $\forall n \in N$:

$$\pi(n)\pi(g)w = \pi(ng)w = \pi(gn')w = \pi(g)(\pi(n')w) \in gW$$

Now since W is irreducible, so is gW since if $W_0 \subset gW$ was an invariant subspace of gW then $g^{-1}W_0$ would be an invariant subspace of W:

$$\forall n \in N, \pi(n)(g^{-1}w_0) = \pi(ng^{-1})w_0 = \pi(g^{-1}n')w_0 = \pi(g^{-1})n'w_0 \in g^{-1}W_0$$

.

Since gW are all irreducible, any two are either equal or disjoint, hence the sum for V is disjoint and so $(\pi|_N, V)$ is a direct sum of the spaces gW.

Proof of (2): Let V_α be the direct sum of all representations isomorphic to W_α so that $V_\alpha \cong \bigoplus_{\beta\in J} W_\alpha$ through an isomorphism ϕ, where β runs through all representations of N isomorphic to W_α. Let π_β be the obvious projections. If L is an irreducible subrepresentation of V_α, then $\pi_\beta \circ \phi(L) \neq 0$ for some β. Then $\pi_\beta \circ \phi(L)$ is a subrepresentation of W_α hence equal to W_α since W_α is irreducible. Since L is not isomorphic to a direct sum, only one $\pi_\beta \circ \phi(L)$ is nonzero, so $L \cong W_\alpha$.

This implies that all V_α are disjoint, and since V is already a sum of irreducible representations through $\sum_{g\in G} gW$, then $V = \bigoplus_{\alpha\in I} V_\alpha$.

Proof of (3):

Let $U_\alpha = \{\sum xW|x \in G, xW \cong W_\alpha\}$. Now we have $V = \sum_{\alpha\in I} U_\alpha$ and $U_\alpha \subset V_\alpha$. Since the V_α are disjoint, we must have $V_\alpha = U_\alpha$.

Now suppose $xW \cong yW$ through ϕ. Letting $\psi = g\phi g^-1$ we get a map $\psi : gxW \to gyW$ that is clearly bijective. We also have $\forall n \in N$:

$$\psi(ngxw) = g\phi((g^{-1}ng)xw) = g(g^{-1}ng)\phi(xw) = n(g\phi g^{-1})(gxw) = n\psi(gxw)$$

Thus $gxW \cong gyW$ through ψ. The two facts above together imply that $\forall\alpha, gV_\alpha \subset V_\beta$ for some β, and that therefore $V_\alpha \subset g^{-1}V_\beta \subset V_\alpha$ since V_α

are disjoint. Comparing the dimensions of these spaces we get that $gV_\alpha = V_\beta$. The action of G must be transitive because any orbit would determine a subrepresentation of V, which is irreducible.

Proof of (4):

Fix an index, say $1 \in I$ and let $H = H_1$. Then by (3) one can find x_α such that $x_\alpha V_1 = V_\alpha$. Note that x_α are coset representatives of H in G. Let $\rho = (\pi|_H, V_1)$. We need to show $\pi \cong Ind_H^G \rho$. Since $V = \bigoplus_{\alpha \in I} V_\alpha$ each $v \in V$ can be represented uniquely as $\sum_{\alpha \in I} x_\alpha v_\alpha$ where $x_\alpha \in V_\alpha$. Now define the map $\phi : v \mapsto \sum_\alpha x_\alpha \otimes v_\alpha$. This is clearly a bijection from V to $Ind_H^G(\rho)$. For each element $g \in G$ we have $gx_\alpha = x_\beta h$ for some β. Now we have:

$$g\phi(x_\alpha v) = g(x_\alpha \otimes v) = x_\beta \otimes hv = \phi(x_\beta hv) = \phi(gx_\alpha v)$$

.

Hence ϕ preserves the action of G and hence is an isomorphism of representations. □

Before we state a corollary, here are some standard definitions:

Definition 2.1. *An irreducible representation is called primitive if it is not induced from any proper subgroup.*

Definition 2.2. *A representation is called isotypic of it is the direct sum of isomorphic irreducible representations.*

Corollary 2.1. *If the representation V of a group G is primitive, then the restriction of V to a normal subgroup is isotypic.*

Proof. In the language of Clifford's theorem, since V is primitive, any V_α must be the entire representation V. In particular this means that all gW are isomorphic and $V|_N$ is the direct sum of all such gW. □

Now we will state, without proof, another result of Clifford that pertains to this case. The proof is found in [Dornhoff, p140]. First we make a definition.

Definition 2.3. *For a group G and a vector space V over a field k. A projective representation is a map $\phi : G \to GL(V)$ such that $\forall x, y \in G$:*

$$\pi(xy) = \alpha(x, y)\pi(x)\pi(y)$$

for some $\alpha(x, y) \in k$.

Irreducibility of a projective representation is defined in the obvious way. Now the result:

Theorem 2.2. *Let V be a vector space over an algebraically closed field k. Let (π, V) be a representation of a group G, and N a normal subgroup of G. Let W be an irreducible subrepresentation of $(\pi|_N, V)$. Let $U = V/W$ as vector spaces. Then there exist irreducible projective representations X and Y:*

$$Y : G \to GL(U) \text{ and } X : G \to GL(W)$$

such that $S(g) = X(g) \otimes Y(g)$ defines an ordinary irreducible represenation of G on $U \otimes_k W$ and $S \cong V$ as representations of G. Furthermore we have $Y|_N = 1_U$.

A note about the proof: This result is proved using Clifford's previous theorem. The key fact is that k is algebraically closed so that $Hom(\pi, \pi) \cong k$ if π is irreducible.

3 Galois representations

Suppose now that k is a complete discrete valuation field of finite residue characteristic p. By G_k we denote the Galois group of the algebraic closure $\bar{k}$, i.e $Gal(\bar{k}/k)$. Let P_k be the wild ramification subgroup of G_k.

The proof of the following theorem can be found in any standard textbook (e.g Dornhoff) and will be ommitted.

Theorem 3.1. *All irreducible representations of supersolvable groups are induced from one-dimensional representations.*

Now we are ready to approach our final result. First a lemma:

Lemma 3.1. *Suppose that a representation T can be written as a tensor product $X \otimes Y$, and that Y is induced from a subrepresentation, then T is similarly induced:*

$$X \otimes Ind(Y') = Ind(Res(X) \otimes Y')$$

Proof. This is clear from the tensor product characterization of induced representations. □

Note that the lemma holds identically for projective representations.

And now the main theorem, cited from [Buhler, p19].

Theorem 3.2. *Let $\mathbb{T} : G_k \to GL(V)$ be a primitive galois representation. Then the restriction of $\mathbb{T}$ to P_k is irreducible.*

Proof. By the corollary to Clifford's theorem, the restriction of $\mathbb{T}$ to P_k is isotypic. Denote by $\mathbb{T}_1$ the irreducible representation correponnding to that restriction. Let T and T_1 denote the projective representations obtained from $\mathbb{T}$ and $\mathbb{T}_1$. Then by Clifford's second theorem we have:

$$T = \bar{T_1} \otimes T_2$$

Where T_2 is an irreducible projective representation that is trivial on P_k, and $\bar{T_1}$ is an extension of T_1 to all of G_k. If $T|_{P_k}$ were reducible, then the degree of T_1 would be strictly smaller than than the degree of T and so the degree of T_2 would be bigger than one. However since T_2 is trivial on P_k, it is a projective representation of G_k/P_k, a supersolvable group. Since all irreducible representations of supersolvable groups are induced, so is T_2 and by the lemma, so is T, which contradicts primitivity. Therefore $\mathbb{T}|_{P_k}$ is irreducible. □

Corollary 3.1. *The degree of* $\mathbb{T}$ *is a power of* p.

Proof. $\mathbb{T}|P_k$ is an irreducible representation of P_k, a pro-finite p-group. Irreducible representations of p-groups are of p-power order. □

4 References

[Brighton] J.W.S Cassels and A. Fröhlich: Algebraic Number Theory. Academic Press, 1967.

[Buhler] Joe.P Buhler: Icosahedral Galois Representations. Springer-Verlag, 1978

[Cassels] J.W.S Cassels: Local Fields. London Mathematical Society, 1986.

[Dornhoff] L. Dornhoff: Group Representation Theory, Part A. Marcel Dekker, Inc. 1971