Dr. Marques Sophie
Office 519

Number theory

Spring Semester 2014

marques@cims.nyu.edu

# Problem Set #9

**Exercise 2:**
If $L/K$ is a Galois extension of algebraic number fields, and $\mathfrak{P}$ a prime ideal which is unramified over $K$ (i.e. $\mathfrak{p} = \mathfrak{P} \cap K$ is unramified in $L$), then there is one and only one automorphism $Frob_{\mathfrak{P}} \in G(L/K)$ such that

$$Frob_{\mathfrak{P}}(a) = a^q mod\ \mathfrak{P}\ \forall a \in B$$

where $q = |k(\mathfrak{p})|$. It is called the **Frobenius automorphism**. The decomposition group $G_{\mathfrak{P}}$ is cyclic and $\phi_{\mathfrak{P}}$ is a generator of $G_{\mathfrak{P}}$.

***Solution:***
*Each $\sigma \in D = D_{\mathfrak{P}}$ acts in a well-defined way on the finite field $k(\mathfrak{P}) = \mathcal{O}_K/\mathfrak{P}$ with $|k(\mathfrak{p})| = p^n = q$ and $|k(\mathfrak{P})| = p^{fn}$, so we obtain a homomorphism*

$$\varphi : D_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})).$$

*We pause for a moment and derive a few basic properties of $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, which are in fact general properties of Galois groups for finite fields. Let $f = [k(\mathfrak{P}) : k(\mathfrak{p})]$. The group $\mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))$ contains the element $Frob_{\mathfrak{P}}$ defined by $Frob_{\mathfrak{P}}(x) = x^q$, because $(xy)^q = x^q y^q$ and $(x+y)^q = x^q + qx^{q-1}y + \cdots + y^q \equiv x^q + y^q \pmod p$. It is well known that the group $k(\mathfrak{P})^*$ is cyclic, so there is an element $a \in k(\mathfrak{P})^*$ of order $p^{nf} - 1$. Then $Frob_{\mathfrak{P}}^m(a) = a^{q^m} = a$ if and only if $(p^{fn} - 1) \mid p^{mn} - 1$ which is the case precisely when $f \mid m$, so the order of $Frob_{\mathfrak{P}}$ is $f$. Since the order of the automorphism group of a field extension is at most the degree of the extension, we conclude that $\mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))$ is generated by $Frob_{\mathfrak{P}}$. Also, since $\mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))$ has order equal to the degree, we conclude that $k(\mathfrak{P})/k(\mathfrak{p})$ is Galois, with group $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ cyclic of order $f$ generated by $Frob_{\mathfrak{P}}$. (Another general fact: Up to isomorphism there is exactly one finite field of each degree. Indeed, if there were two of degree $f$, then both could be characterized as the set of roots in the compositum of $x^{p^{nf}} - 1$, hence they would be equal.)*

*Suppose that $L/K$ is a finite Galois extension with group $G$ and $\mathfrak{p}$ is a prime ideal such that $e = 1$ (i.e., an unramified prime ideal). Then $I_{\mathfrak{P}} = 1$ for any $\mathfrak{P} \mid \mathfrak{p}$, so the map $\varphi$ is a canonical isomorphism $D_{\mathfrak{P}} \cong Gal(k(\mathfrak{P})/k(\mathfrak{p}))$. By what we have done before, the group $Gal(k(\mathfrak{P})/k(\mathfrak{p}))$ is cyclic with canonical generator $Frob_{\mathfrak{P}}$. The corresponding to $\mathfrak{P}$ is $Frob_{\mathfrak{P}} \in D_{\mathfrak{P}}$. It is the unique element of $G$ such that for all $a \in \mathcal{O}_K$ we have $Frob_{\mathfrak{P}}(a) \equiv a^q \pmod{\mathfrak{p}}$., the unicity comes from the isomorphism $D_{\mathfrak{P}} \simeq Gal(k(\mathfrak{P})/k(\mathfrak{p}))$ since $Frob_{\mathfrak{P}}(0) = 0 \pmod{\mathfrak{p}}$ implies that $Frob_{\mathfrak{P}}(\mathfrak{P}) = \mathfrak{P}$.*

**Exercise 1:**
If $L/K$ is a Galois extension of algebraic number fields with noncyclic Galois group, then there are at most finitely many non split prime ideals of $K$.
***Solution:***
*Let $G = Gal(L/K)$, $\mathfrak{p}$ prime ideal of $\mathcal{O}_K$. Suppose $\mathfrak{p}$ is unramified and nonsplit. (Since only finitely many primes are ramified, it suffices to show that this cannot occur.) Since $\mathfrak{p}$ is unramified and nonsplit and $efg = |G|$, we see that $f = |G|$ and the decomposition group $D_\mathfrak{p}$ is isomorphic to $G$. But we also have that $D_\mathfrak{p}$ is isomorphic to the Galois group of the residue field of $L/K$ at $\mathfrak{p}$, which is cyclic of order $f$. This contradicts our hypothesis on $G$.*

**Exercise 5:**
Let $L/K$ be a solvable extension of prime degree $p$ (not necessarily Galois). If the unramified prime ideal $\mathfrak{p}$ in $L$ has two prime factors $\mathfrak{P}$ and $\mathfrak{P}'$ of degree 1, then it is already totally split.
Hint: Use the following result of Galois: if $G$ is a transitive solvable permutation group of degree $p$, then there is no nontrivial permutation $\sigma \in G$ which fixes two distinct letters.
***Solution:***
*Let $\mathcal{O}_K$ be a Dedekind domain, $L$ the fraction field of $\mathcal{O}_K$. Let $L/K$ be a finite, separable extension, not necessarily Galois, of degree $p$. Let $N$ be the normal closure of $L/K$. Let $G = Gal(N/K)$ and $H = Gal(N/L)$. Let $\mathfrak{p}$ be a prime of $K$ (i.e. of $\mathcal{O}_K$). Let $\mathfrak{P}$ be a prime of $N$ above $\mathfrak{p}$. Let $G_\mathfrak{P}$ denote the decomposition group of $\mathfrak{P}$ over $K$. Then, there is a bijection from the set of double cosets $H\backslash G/G_\mathfrak{P}$ to the set $P_\mathfrak{p}$ of primes of $L$ above $\mathfrak{p}$, given by:*

$$H\backslash G/G_\mathfrak{P} \to P_\mathfrak{p},\ H\sigma G_\mathfrak{P} \mapsto \sigma\mathfrak{P} \cap L$$

*Now suppose the prime $\mathfrak{p}$ is unramified in $L$. Then $\mathfrak{p}$ is also unramified in $N$.*
*Note that there are $p$ cosets $H\sigma_1, ..., H\sigma_n$ of $H\backslash G$ where $n = [L : K]$. There is an action of $G$ that permutes the cosets $H\sigma_i$ by right multiplication. They key observation is this: The size of the orbit of the coset $H\sigma_i$ under the right action of the decomposition group $G_\mathfrak{P}$ equals the inertia degree of the prime $\sigma_i\mathfrak{P} \cap L$ over $\mathfrak{p}$.*
*To show this, first observe that, for $\rho \in G_\mathfrak{P}$ and $\sigma_i \in G$,*

$$H\sigma_i\rho = H\sigma_i \Leftrightarrow \rho \in \sigma_i^{-1} H_{\sigma_i(\mathfrak{P})}\sigma_i$$

*where $H_{\sigma_i(\mathfrak{P})}$ is the decomposition group of $\sigma_i(\mathfrak{P})$ over $L$.*
*Thus the size of the orbit of $H\sigma_i$ is*

$$[G_\mathfrak{P} : Stab(H\sigma_i)] = [G_\mathfrak{P} : \sigma_i^{-1} H_{\sigma_i(\mathfrak{P})}\sigma_i] = [\sigma_i G_\mathfrak{P} \sigma_i^{-1} : H_{\sigma_i(\mathfrak{P})}] = [G_{\sigma_i(\mathfrak{P})} : H_{\sigma_i(\mathfrak{P})}]$$

*$[G_{\sigma_i(\mathfrak{P})} : H_{\sigma_i(\mathfrak{P})}]$ equals the inertia degree of $\sigma_i(\mathfrak{P} \cap L$ over $\mathfrak{p}$, proving the highlighted claim above.*
*Now assume the degree $p$ of $L/K$ is prime, and assume that $\mathfrak{p}$ has two prime factors $\mathfrak{P}_1$ and $\mathfrak{P}_2$ in $L$ of degree 1. This implies we have two cosets $H\sigma_1$ and $H\sigma_2$ who orbits under the action of $G_\mathfrak{P}$ are of size 1. $G$ is a solvable group with a transitive action on*

*the $p$ cosets $H\sigma_1$,...,$H\sigma_p$. Thus each element of $G_{\mathfrak{P}}$ fixes the two cosets $H\sigma_1$ and $H\sigma_2$, so by the theorem given in the Hint, each element of $G_{\mathfrak{P}}$ must fix all the cosets, so $G_{\mathfrak{P}}$ partitions the $H\sigma_i$ into $p$ distinct orbits of one element each. Thus, every prime factor of $\mathfrak{p}$ in $L$ is of degree 1 over $\mathfrak{p}$.*

**Exercise:**
Let $L/K$ be a normal finite extension of finite fields of characteristic $p$ and $L^s/K$ the maximal separable sub extension. Prove that

$$G(L/K) = G(L^s/K)$$

***Solution:***
*We know that $|G(L/K)| \geq |G(L^s/K)|$.*
*Since a element of $G(L/K)$ send a separable element to a separable element it induces by restriction an element of $G(L^s/K)$. This permits to define the morphism:*

$$\begin{array}{cccc} \Phi: & G(L/K) & \rightarrow & G(L^s/K) \\ & \sigma & \mapsto & \sigma|_{L^s} \end{array}$$

*We will prove that $\Phi$ is injective so that $|G(L/K)| = |G(L^s/K)| < \infty$ and we have an isomorphism.*
*For if, we have to prove that if $\sigma \in G(L/K)$ is such that $\sigma(a) = a$ , for any $a \in L^s$, then we want to prove that for any $u \in L \backslash L^s$ $\sigma(u) = u$. But since $L/K$ is normal, then $L/L^s$ is purely inseparable, but then for any $u \in L$, there is a $n$, such that $u^{p^n} \in L^s$, so that $\sigma(u^{p^n}) = u^{p^n}$ and $(\sigma(u)^{p^n} = u^{p^n}$, which implies $\sigma(u) = u$, by injectivity of the Frobenius element. We also have the surjectivity of the map from the normality of $L/K$.*