Dr. Marques Sophie
Office 519

Spring Semester 2014
marques@cims.nyu.edu

Problem Set #8

Exercise 4 p 53

A prime ideal $\mathfrak{p}$ of K is totally split in the separable extension L/K if and only if it is totally split in the Galois closure N/K of L/K.

Solution:

Let L/K be a separable extension and denote by N/K "its" Galois closure G. In G, consider the subgroup $H = G(N|L)$.

Claim: *Let $\mathfrak{p}$ be a prime ideal of K and $P_{\mathfrak{p}}$ be the set of all the prime ideal of L above $\mathfrak{p}$. If $\mathfrak{P}$ is a prime ideal of N above $\mathfrak{p}$.*

One can define a map

$$\begin{array}{rccc} \phi : & H\backslash G/G_{\mathfrak{P}} & \to & P_{\mathfrak{p}} \\ & H\sigma G_{\mathfrak{P}} & \mapsto & \sigma\mathfrak{P} \cap L \end{array}$$

and it is a bijection of sets.

Proof of the claim

First, ϕ is well-defined. Indeed, let τ and $\sigma \in G$, suppose that $H\sigma G_{\mathfrak{P}} = H\tau G_{\mathfrak{P}}$. Then, there is $h \in H$ and $g \in G_{\mathfrak{P}}$ such that $\tau = h\sigma g$, so that

$$(\tau\mathfrak{P}) \cap L = (h\sigma g\mathfrak{P}) \cap L = h(\sigma\mathfrak{P}) \cap L = \sigma\mathfrak{P} \cap L$$

In fact, by definition H fixes L and g stabilizes $\mathfrak{P}$ being in the decomposition group of $\mathfrak{P}$ Then,

$$\phi(H\sigma G_{\mathfrak{P}}) = \phi(H\tau G_{\mathfrak{P}})$$

Also, ϕ is surjective. Indeed, let $\mathfrak{q} \in P_{\mathfrak{p}}$, we want to find σ such that $\phi(H\sigma G_{\mathfrak{P}}) = \mathfrak{q}$ i.e. $\sigma(\mathfrak{P}) \cap L = \mathfrak{q}$. Let $\mathfrak{Q}$ be a prime ideal above $\mathfrak{q}$. So that

$$\mathfrak{Q} \cap K = \mathfrak{q} \cap K = \mathfrak{p}$$

So, $\mathfrak{Q}$ and $\mathfrak{P}$ are prime ideal in the Galois extension N/K above $\mathfrak{p}$. As a consequence, there is $g \in G$ such that $g\mathfrak{P} = \mathfrak{Q}$ and $\phi(H\sigma G_{\mathfrak{P}}) = \sigma(\mathfrak{P}) \cap L = \mathfrak{Q} \cap L = \mathfrak{q}$.

Finally, ϕ is injective. Suppose that for some σ, $\tau \in G$, $\phi(H\sigma G_{\mathfrak{P}}) = \phi(H\tau G_{\mathfrak{P}})$, i.e. $\sigma(\mathfrak{P}) \cap L = \tau(\mathfrak{P}) \cap L = \mathfrak{q}$. We want to prove that $H\sigma G_{\mathfrak{P}} = H\tau G_{\mathfrak{P}}$. Since $\sigma(\mathfrak{P})$ and $\tau(\mathfrak{P})$ are two prime ideal over ıı, there is $h \in H$ such that $h\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$ and then $\tau^{-1}h\sigma(\mathfrak{P}) = \mathfrak{P}$ that is $\tau^{-1}h\sigma \in G_{\mathfrak{P}}$ so that $h\sigma g^{-1} = \tau$ and $H\sigma G_{\mathfrak{P}} = H\tau G_{\mathfrak{P}}$ and this prove the claim.

Recall that a prime ideal is totally split in some Galois extension it decomposition group is trivial.

Suppose that $\mathfrak{p}$ is a prime ideal totally split in K, the $G_{\mathfrak{P}}$, so that

$$|H\backslash G/G_{\mathfrak{P}}| = [G : H] = [L : K] = |P_{\mathfrak{p}}|$$

so that $\mathfrak{p}$ is totally split in L.
Conversely, if $\mathfrak{p}$ split completely in L, then the number of double cosets $H\backslash G/G_{\mathfrak{P}}$ equals $[L:K]=[G:H]$; this is the same as the number of right cosets of H; since each double coset decomposes as a disjoint union of right cosets of H,

$$H\sigma G_{\mathfrak{P}} = \coprod_{g\in G_{\mathfrak{P}}} H\sigma g$$

It follows that $H\sigma G_{\mathfrak{P}} = H\sigma$ for all $\sigma \in G$ and in particular all conjugates of $G_{\mathfrak{P}}$ are contained in H. That is, the normal subgroup $N(G_{\mathfrak{P}})$ generated by $G_{\mathfrak{P}}$ is contained in H.
But now, if F is the fixed field of N by the action of $N(G_{\mathfrak{P}})$, by Galois theory the extension F/K is Galois so by definition of the Galois closure $F=N$.

Exercise 5 p 53
For a number field K, the statement of proposition (8.3) concerning the prime decomposition in the extension $K(\theta)$ holds for all prime ideals $\mathfrak{p} \nmid (B : A[\theta])$.
Solution:
Let $L=K(\theta)$ with $\theta \in B$ and p a prime number. We construct the homomorphism:

$$\begin{array}{rccc} \theta: & A[\theta]/pA[\theta] & \to & B/pB \\ & x+pA[\theta] & \mapsto & x+pB \end{array}$$

Clearly well defined. Suppose $p \nmid m = [B : A[\theta]]$ (this index is finite and B and $A[\theta]$ have equal rank). Pick an $\tilde{m}$ for which $\tilde{m}m \equiv 1 \bmod p\mathbb{Z}$ (hence mod pB too). If $x \in B$ is arbitrary then we know that $mx \in A[\theta]$ (consider the finite quotient group $B/A[\theta]$) hence $\tilde{m}mx + pA[\theta] \mapsto x + pB$, so we know the map is surjective. Both quotients are finite groups of size p^n where $n = [K(\theta) : K]$, so the map must be an isomorphism. Therefore, we have

$$B/pB \simeq A[\theta]/pA[\theta] \simeq A[T]/(p, p(T)) \simeq \mathbb{F}_p[T]/(p(T))$$

where $f(T)$ is the minimal polynomial of θ (monic and integer coefficients).
Suppose pB and $f(T) \in \mathbb{F}_p[T]$ factor into prime ideals and irreducibles respectively as

$$pB = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_g^{e_g}, \quad \bar{p}(T) = \bar{p_1}(T)^{r_1} .... \bar{p_h}(T)^{r_h}$$

By Chinese Remainder Theorem,

$$B/pB \simeq \prod_{i=1}^{g} B/\mathfrak{p}_i^{e_i}, \quad \mathbb{F}_p[T]/(\bar{p}(T)) \simeq \prod_{j=1}^{h} \mathbb{F}_p[T]/(\bar{p_i}(T)^{r_i})$$

A maximal ideal of a direct product is one in which all but one of the summands may contain anything, and that one coordinate contains elements from a maximal ideal of that summand's ring; Futhermore a maximal ideal of B/P^{μ} corresponds to a maximal ideal of B containing P^{μ}, which must be P for B, $\mathbb{F}_p[T]$ and $P = \mathfrak{P}_i, (\bar{p_i}(T))$ resp. Therefore

$$\{\mathfrak{p}|p\} \simeq MaxSpec(B/pB) \simeq MaxSpec(\mathfrak{F}_p[T]/(\bar{p}(T))) \simeq \{\pi|\bar{p}\}$$

is a natural bijection. In particular, this means $g = h$ (taking cardinalities above). Futhermore, the data e_i and r_i can respectively be read off the factors $B/\mathfrak{p}_i^{e_i}$ and $\mathbb{F}_p[T]/(\bar{p}_i(T))^{r_i}$ as the nilpotent of their unique maximal ideals, and the data f_i and $deg(p_i)$ can be read off of the size of their unique residue fields. Yet further, if we pull back $(\bar{p}_i(T))$ through the isomorphism and then lift back to B we obtain $\mathfrak{p}_i = (p, p_i(\theta))$.

Exercise 7 p 53

Let $(a, p) = 1$ and $a\nu = r_\nu \; modp$, $\nu = 1, ..., p-1$, $0 < r_\nu < p$. Then the r_ν give a permutation π_a of the number 1, ... $p-1$. Show that $sgn(\pi_a) = \left(\frac{a}{p}\right)$.

Solution:

We can show that there is a unique non-constant morphism of group from $(\mathbb{Z}/p\mathbb{Z})^*$ to $\{\pm 1\}$ in fact it is determined by the image of the generator which must be -1 since the morphism is not constant. We can check easily that the maps $a \mapsto sgn(\pi_a)$ and $a \mapsto \left(\frac{a}{p}\right)$ are such morphisms and that they are not constant since there is always non-square mod p and $a = \xi$ a primitive root of unity leads to $sgn(\pi_\xi) = -1$. As a consequence, they are equals.

Or

Note that for any a, b coprime with p, we have $\pi_a \pi_b = \pi_{ab}$.
Let $\zeta \in \mathbb{F}_p^*$ be a primitive element. Then $\mathbb{F}_p^* = \{1, \zeta, ..., \zeta^{p-2}\}$.
Let a be an integer coprime with p, then there is $i \in \{1, ..., p_1\}$ such that $a = \zeta^{i-1}$. Now, we observe that σ_ζ is the cycle $(1, \zeta, ..., \zeta^{p-2})$ whose parity is $(-1)^{(p-1)-1} = (-1)^{p-2} = -1$ since p is odd. Then $sgn(\pi_a) = sgn(\pi_\zeta^j) = sgn(\pi_\zeta)^j = (-1)^j$ (Here we use the multiplicativity of sgn.
Now $\left(\frac{a}{p}\right) \equiv \zeta^{j(p-1)/2}$ mod p, by Euler criterion. But $\zeta^{(p-1)/2} = -1$ mod p ζ being a primitive root, So that $\left(\frac{a}{p}\right) = (-1)^j = sgn(\pi_a)$.

Exercise 9 p 53

Study the Legendre symbol $\left(\frac{3}{p}\right)$ as a function of $p > 3$. Show that the property of 3 being a quadratic residue or non-residue mod p depends only on the class of p mod 12.

Solution:

Let p be a prime $p > 3$, so that $gcd(p, 3) = 1$.
By quadratic reciprocity:

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(3-1)/2 \cdot (p-1)/2} = (-1)^{(p-1)/2}$$

Trivially, $\left(\frac{1}{3}\right) = 1$ and $\left(\frac{2}{3}\right) = -1$.
As a consequence, if $p \equiv 1$ mod 3 then $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}$. So that $\left(\frac{3}{p}\right)$ depends only on the parity of $(p-1)/2$. More precisely, $\left(\frac{3}{p}\right) = -1$ if $(p-1)/2$ is odd, that is $p \equiv 3$ mod4 and $\left(\frac{3}{p}\right) = 1$ if $(p-1)/2$ is even, that is $p \equiv 1$mod4.
Now, if $p \equiv -1$ mod 3 then $\left(\frac{3}{p}\right) = -(-1)^{(p-1)/2}$. Again, $\left(\frac{3}{p}\right)$ depends only on the parity of $(p-1)/2$. More precisely, $\left(\frac{3}{p}\right) = -1$ if $(p-1)/2$ is even, that is $p \equiv 1$ mod4 and

$\left(\frac{3}{p}\right) = 1$ *if* $(p-1)/2$ *is odd, that is* $p \equiv -1 mod 4$.
In summary, using chinese remainder, We get $\left(\frac{3}{p}\right) = 1$ *if and only if* $p \equiv \pm 1$ *mod* 12.
As a consequence $\left(\frac{3}{p}\right) = -1$ *if and only if* $p \equiv \pm 5$ *mod* 12.