EXERCISE SHEET 4: ALGEBRAIC NUMBER THEORY SUMMER SCHOOL AT AMSS 2019

Exercise 1. Use the cyclotomic extension $\mathbb{Q}(\zeta_8)$ to show the quadratic reciprocity law for 2: if p is an odd prime, 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 8$.

Exercise 2. Let $K = \mathbb{Q}(\zeta_{25})$.

(1) Prove that K has a unique subfield M of degree 5 over $\mathbb{Q}$, and find an explicit $\alpha \in K$ such that $M = \mathbb{Q}(\alpha)$.
(2) Find the decompositions of the primes $p = 2, 3, 5$ in $M/\mathbb{Q}$, and their corresponding decomposition subfields.
(3) Prove that p splits in M if and only if $p \equiv \pm 1, \pm 7 \mod 25$.

Exercise 3. (1) Prove that there exists a unique cubic Galois extension $K/\mathbb{Q}$ which is unramified outside 13. (*Hint: use Kronecker–Weber's theorem.*)
(2) Find an explicit irreducible cubic polynomial $f(T) \in \mathbb{Q}[T]$ such that $K = \mathbb{Q}[T]/(f(T))$.

Exercise 4. In this exercise, we provide an elementary argument to show a weaker version of a special case of Chebotarev density theorem.

(1) Let $f(X) \in \mathbb{Z}[X]$ be a non-constant polynomial. Prove that there exist infinitely many primes p such that the image of $f(X)$ in $\mathbb{F}_p[X]$ has a root in $\mathbb{F}_p$.
Hint: Consider the prime factors of $f(n!a_0)$ for some large n with $a_0 = f(0)$.
(2) Show that given an integer $N \geqslant 3$, there exist infinitely many primes p such that $p \equiv 1 \mod N$.
Hint: Apply (1) to the cyclotomic polynomial $\Phi_N(X)$.

Exercise 5. Let $f(X) \in \mathbb{Z}[X]$ be a nonconstant polynomial. For a prime number p, let $n(p)$ be the number of distinct zeros of $(f \mod p)$ in $\mathbb{F}_p$. Prove that the average of $n(p)$, taken over all prime numbers p, is equal to the number of distinct monic irreducible factors of f in $\mathbb{Q}[X]$. (*Hint: Your solution should include a rigorous definition of that average.*)

Solution. The first step is to reduce the problem to the case when $f(x)$ is irreducible. Write $f(x) = \prod_i f_i(x)^{e_i}$ with each $f(x)$ irreducible in $\mathbb{Q}[x]$. Then $n_f(p) = \sum_i n_{f_i}(p)$. So if we can show

$$\lim_{t \to +\infty} \frac{\sum_{p \leq t} n_{f_i}(p)}{\sum_{p \leq t} 1} = 1$$

for each $f_i(x)$, then we are done.

We assume thus $f(x)$ is irreducible. Let $K = \mathbb{Q}[x]/(f(x))$ and $L/\mathbb{Q}$ be its Galois closure with Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/K)$. The number of roots of $f(x) \mod p$ is in bijection with the number of degree 1 primes of K lying above p. Let $\mathfrak{p}$ be a prime of L above p, which is unramified in L, and $\mathfrak{p}_K = \mathfrak{p} \cap K$. Then $f(\mathfrak{p}_K|p) = 1$ if and only if the Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in G$ actually lies in H. Assume this is the case, then for another prime $\mathfrak{p}' = \sigma(\mathfrak{p})$ of L with $\sigma \in G$, $\mathfrak{p}' \cap K = \mathfrak{p}_K$ if and only if $\sigma \in H$. So the number of degree 1 primes in K above p which lie in the same G-conjugacy class as $\mathrm{Frob}_{\mathfrak{p}}$ is given by

$$\frac{\#\{\sigma \in G | \sigma \mathrm{Frob}_{\mathfrak{p}} \sigma^{-1} \in H\}}{\# H}.$$

Let H/C_G denote the equivalence class of H under the conjugate action by G, i.e. two elements $h_1, h_2 \in H$ are equivalent in H/C_G if there exists $\sigma \in G$ such that $\sigma h_1 \sigma^{-1} = h_2$. For each $[h] \in H/C_G$, the density of primes p such that the G-conjugacy class of Frobenii at p is the same as h is given by

$$\frac{\#\{g \in G | g \text{ conjugate to } h\}}{\# G} = \frac{1}{\# Z_h(G)},$$

where $Z_h(G)$ is the centralizer of h in G. So the limit above is finally given by

$$\begin{aligned} &\sum_{[h] \in H/C_G} \frac{1}{\# Z_h(G)} \frac{\#\{\sigma \in G | \sigma h \sigma^{-1} \in H\}}{\# H} \\ &= \sum_{[h] \in H/C_G} \frac{\#\{h' \in H | \exists \sigma \in G, h' = \sigma h \sigma^{-1}\}}{\# H} \\ &= \sum_{h \in H} \frac{1}{\# H} = 1. \end{aligned}$$

Another explanation using the Dirichlet density is the following. Assume still $f(x)$ irreducible, and let K be as above. Then

$$\sum_p \frac{n_f(p)}{p^s} = \sum_{\mathfrak{p} \subset \mathcal{O}_K, f(\mathfrak{p}|p) = 1} \frac{1}{N(\mathfrak{p})^s}.$$

But it is well known that

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \subset \mathcal{O}, f(\mathfrak{p}|p)=1} \frac{1}{N(\mathfrak{p})^s}}{\log(\frac{1}{s-1})} = 1.$$

$\square$