Math 204A (Number Theory), UCSD, fall 2020
Problem Set 6 – due Thursday, November 19, 2020

1. (a) Let $N \geq 3$ be an integer and let Φ_N be the N-th cyclotomic polynomial. Prove that for every integer m, every prime divisor of $\Phi_N(m)$ not dividing N is congruent to 1 modulo N.

   (b) In class, I stated that for every number field K, there exist infinitely many primes p which split completely in K. Prove this for the cyclotomic field $K = \mathbb{Q}(\zeta_N)$ *without* using Dirichlet or Chebotarev. (Hint: suppose there are only finitely many, take their product...)

2. Let L/K be an extension of number fields with Galois closure M. Let $\mathfrak{p}$ be a prime of K.

   (a) Prove that if $\mathfrak{p}$ is unramified in L, then it is unramified in M also.

   (b) Prove that if $\mathfrak{p}$ is unramified and totally split in L, then it is totally split in M also.

   (Hint for both parts: put $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. Pick a prime $\mathfrak{q}$ of M above $\mathfrak{p}$ and consider how $G_{\mathfrak{q}}$ or $I_{\mathfrak{q}}$ intersects the various conjugates of H.)

3. Let m be an integer which is not a perfect square, and put $K = \mathbb{Q}(m^{1/4})$. Let L be the Galois closure of $K/\mathbb{Q}$. Let p be an odd prime not dividing m and let $\mathfrak{q}$ be a prime above p in L. For each possible value for the decomposition group $G_{\mathfrak{q}}$, describe the corresponding splitting of p in K.

4. (a) Let k be a field. Prove that the ring of formal power series $k[\![t]\!]$ is a discrete valuation ring.

   (b) Prove that the subring of $\mathbb{R}[\![t]\!]$ consisting of power series with positive radius of convergence is a discrete valuation ring.

5. Prove that for every finite abelian group A, there exists a Galois number field K with $\mathrm{Gal}(K/\mathbb{Q}) \cong A$. (Hint: find K inside a suitable cyclotomic number field. Remember that A is a product of cyclic groups.)