Math 620 – Fall 2024 – Harry Tamvakis

PROBLEM SET 5 – Due November 7, 2024

1) (a) Let n be a positive integer and let $\Phi_n(x)$ be the n-th cyclotomic polynomial. Let a be any integer. Show that if p is a prime that divides $\Phi_n(a)$, then either p divides n or $p \equiv 1 \pmod{n}$.

(b) Prove that for every natural number n, there are infinitely many prime numbers $p \equiv 1 \pmod{n}$ by arguing as follows. Suppose that there are only finitely many such primes and let m be their product. Choose x sufficiently large so that $\Phi_n(mnx) \neq 1$, and use (a) to arrive at a contradiction. (This is a special case of Dirichlet's prime number theorem).

(c) Prove that for every finite abelian group G, there exists a Galois extension $K/\mathbb{Q}$ with Galois group $G(K/\mathbb{Q}) \cong G$. The same problem without the word 'abelian' is a famous open question.

2) Let $|\cdot|$ be a nonarchimedean absolute value on a field K.

(a) Define the open disk with center $a \in K$ and radius $r > 0$ to be the set

$$D(a,r) := \{x \in K \,:\, |x-a| < r\}.$$

Prove that if two open disks intersect, then one of them must contain the other. Prove also that the circumference $\{x \in K \,:\, |x-a| = r\}$ of $D(a,r)$ is a disjoint union of open disks of radius r. Show that $D(a,r)$ is both an open and closed set in the topology determined by $|\cdot|$.

(b) Assume that $(K, |\cdot|)$ is complete. Prove that the series $\sum_{n=1}^{\infty} a_n$ converges if and only if $\lim a_n = 0$.

3) Let p and q be rational primes. Prove that the field $\mathbb{Q}_p$ is isomorphic to the field $\mathbb{Q}_q$ if and only if $p = q$.

4) (a) Prove that the p-adic power series $\displaystyle\sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$ for $\log(1+x)$ converges in $\mathbb{Q}_p$ for $|x| < 1$ and diverges elsewhere. This allows one to define a p-adic logarithm $\log_p(x) := \log[1+(x-1)]$.

(b) Prove that $\log_p(xy) = \log_p(x) + \log_p(y)$ for all $x, y \in 1 + p\,\mathbb{Z}_p$.

5) (a) Show that the p-adic valuation of $n!$ is at most $\dfrac{n}{p-1}$.

(b) Show that the p-adic valuation of $(p^m)!$ is equal to $\dfrac{p^m - 1}{p-1}$.

(c) Prove that the exponential series $\displaystyle\sum_{n=0}^{\infty} \frac{x^n}{n!}$ converges for $|x| < p^{-1/(p-1)}$ and diverges elsewhere.

Remark: Since the valuation v on $\mathbb{Q}_p$ is discrete and $0 < 1/(p-1) < 1$, there is no $x \in \mathbb{Q}_p$ such that $v(x) = 1/(p-1)$. Hence $|x| < p^{-1/(p-1)}$ is equivalent to $|x| < 1$. However the sharper bound in the problem is useful in situations where $\mathbb{Q}_p$ is embedded in a larger field which extends the p-adic absolute value.