MATH 254 A: PROBLEM SET 5

MARTIN OLSSON

Due Wed Oct 15

(1) Let G be a finite group and let $\chi : G \to \mathbb{C}^*$ be a homomorphism. Show that

$$\sum_{g\in G} \chi(g)$$

is zero unless $\chi(g) = 1$ for all g in which case the sum is equal to the order of G.

(2) Define the *n-th cyclotomic polynomial* $\Phi_n(X)$ to be the irreducible polynomial of a primitive n-th root of unity ζ_n, so

$$\Phi_n(X) = \prod_{(j,n)=1} (X - \zeta_n^j).$$

(a) Show that

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

(b) Suppose p is a prime not dividing n. Show that p divides $\Phi_n(a)$ for some integer $a \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{n}$.

(c) Show that for any integer $n \geq 1$ there are infinitely many primes p with $p \equiv 1 \pmod{n}$ (hint: Suppose there are only finitely many $p_1, \ldots, p_r$, set $M = np_1 \cdots p_r$ and consider $\Phi_n(NM)$ for N large).

(3) Let p be an odd prime, and let ζ_p be a primitive p-th root of unity.

(a) Show that $\mathbb{Q}(\zeta_p)$ contains a quadratic subfield.

(b) Using what we know about ramification in quadratic fields, show that this quadratic subfield must be $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod{4}$ and $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod{4}$.

(4) Let ζ_n be a primitive n-th root of unity. Show that the only roots of unity in $\mathbb{Q}(\zeta_n)$ are those of the form $\pm\zeta_n^j$.