Silvain Rideau
1091 Evans

silvain.rideau@berkeley.edu
`www.normalesup.org/~srideau/en/teaching`

Homework 10

Due November 29th

The questions indicated as (Harder) are optional and will not be taken in account in the grade.

Problem 1 :

1. Let $P_n = X^n - 1$. Let $\mu_n \subseteq \mathbb{C}$ be the set of roots of P_n in $\mathbb{C}$. The elements of μ_n are called the n-th roots of the unity. Show that
$$P_n = \prod_{\zeta\in\mu_n} X - \zeta.$$
2. A $\zeta \in \mu_n$ is said to be primitive if it is not a d-th root of the unity for any $d < n$. Show that there are $\varphi(n)$ primitive n-th roots of the unity, where $\varphi(n)$ is Euler's totient function.
3. Let
$$\Phi_n(X) = \prod_{\zeta\in\mu_n \text{ primitive}} X - \zeta.$$
Show that $P_n = \prod_{d|n} \Phi_d$. Conclude that $\Phi_n(X) \in \mathbb{Z}[X]$.
4. (Harder) Let p be a prime number. Show that $\Phi_p(X+1)$ is irreducible in $\mathbb{Z}[X]$. Conclude that Φ_p is irreducible in $\mathbb{Z}[X]$.

Problem 2 :
Let K be a field. For all $n \in \mathbb{Z}$, let $\overline{n} = n \cdot 1_K \in K$. For all $P = \sum_{i=0}^n c_i X^i \in \mathbb{Z}[X]$, let $\overline{P} = \sum_{i=0}^n \overline{c_i} X^i \in K[X]$.

1. Show that, if $a \in K^\star$ is order n, then $\overline{\Phi}_n(a) = 0$.
2. Until the end of that problem, we will assume that $|K| = q < \infty$. Show that there are at most $\sum_{d|q-1, d<q-1} \deg(\Phi_d)$ elements in $K^\star$ which are not order $q-1$.
3. Show that $K^\star$ is cyclic.

Problem 3 :
Recall that $\mathbb{Z}[i]$ is the subring of $\mathbb{C}$ consisting of elements of the form $a + ib$ where a, $b \in \mathbb{Z}$. Let $p \in \mathbb{Z}$ be prime. Recall that $\mathbb{Z}[i]$ is a Euclidian domain.

1. Show that $\mathbb{Z}[X]/(p, X^2+1)$, $\mathbb{Z}[i]/(p)$ and $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ are isomorphic.
2. Assume that $p \neq 2$, show that the following are equivalent:
   a) -1 is a square in $(\mathbb{Z}/p\mathbb{Z})$;
   b) there is an element of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\star$;
   c) $4|p-1$.
3. Assume that $p = xy$ for some x, $y \in \mathbb{Z}[i]$. Show that $|x|^2 \in \{1, p, p^2\}$, here $|x|$ denotes the complex norm.

4. Show that the following are equivalent:
   a) $p = 2$ or $p \equiv 1 \mod 4$;
   b) p is reducible in $\mathbb{Z}[i]$;
   c) there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.
5. (Harder) Pick any $x = \prod_i p_i^{\alpha_i} \in \mathbb{Z}_{>1}$ where $\varepsilon \in \{-1, 1\}$, $\alpha_i \in \mathbb{Z}_{>0}$ and the p_i are distinct primes. Show that there exists $a, b \in \mathbb{Z}$ such that $x = a^2 + b^2$ if and only if for all i such that α_i is odd, $p_i \not\equiv 3 \mod 4$.