nyt
Silvain Rideau
1091 Evans

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

Final (Lecture 002)

May 11th

- To do a later question, you can always assume a previous question even if you have not answered it.
- There are three problems (the third one is on the other side of this page).
- I know this is long. I don't expect you to do everything. My guess is that people doing between ten and twelve questions will get a top grade.

Fact 0.1:
In the following problems, we will be assuming that the following are true (you do NOT have to prove them):

- *For all $d \in \mathbb{Z}_{>0}$, there exists a non constant monic polynomial $\Phi_d(X) \in \mathbb{Z}[X]$ such that $X^n - 1 = \prod_{d|n} \Phi_d(X)$;*
- *For all q, $d \in \mathbb{Z}_{>1}$, $|\Phi_d(q)| > q - 1$. Here $|\Phi_d(q)|$ denotes the absolute value.*

Problem 1 :
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 $P \mapsto \overline{P}$ is a (unitary) ring homomorphism from $\mathbb{Z}[X]$ to $K[X]$.
2. Show that, if $a \in K^\star$ is order n, then $\overline{\Phi}_n(a) = 0$.
3. 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 $q - 1$.
4. Show that $K^\star$ is cyclic.

Problem 2 :
Recall that $\mathbb{Z}[i]$ is the subring of $\mathbb{C}$ consisting of elements of the form $a + ib$ where a, $b \in \mathbb{Z}$. Recall that $\mathbb{Z}[i]$ is a Euclidian domain. Let $p \in \mathbb{Z}$ be prime.

1. Show that $\mathbb{Z}[X]/(p, X^2 + 1)$, $\mathbb{Z}[i]/(p)$ and $\mathbb{F}_p[X]/(X^2 + 1)$ are isomorphic.
2. Assume that $p \neq 2$, show that the following are equivalent:
   a) -1 is a square mod p;
   b) there is an element of order 4 in $\mathbb{F}_p^\star$;
   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 $p = 1 \mod 4$;
   b) p is reducible in $\mathbb{Z}[i]$;
   c) there exist a, $b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

Problem 3 :
Let D be a division ring.

1. Let $F = \{x \in D : \forall y \in D, xy = yx\}$. Show that F is a field.

2. Until the end of that problem, we will assume that $|D| < \infty$. Let $q = |F|$, show that there exists $m \in \mathbb{Z}_{>0}$ such that $|D| = q^m$.

3. Pick any $d \in D$. Show that $\mathrm{C}_D(d) = \{x \in D : xd = dx\} \subseteq D$ is a subring of D containing F, that it is a division ring and that there exists an $m_d \in \mathbb{Z}_{>0}$ such that $|\mathrm{C}_D(d)| = q^{m_d}$.

4. Show that there exists $d_i \in D$ for $i = 1 \dots k$, such that
$$q^m - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^m - 1}{q^{m_{d_i}} - 1}.$$

5. Show that for all $n < m$, $\frac{q^m-1}{q^n-1} \in \mathbb{Z}$ if and only if $n|m$. When $n|m$, show that $\Phi_m(q)|\frac{q^m-1}{q^n-1}$ in $\mathbb{Z}$.

6. Show that $\Phi_m(q)|q-1$.

7. Conclude that D is a field.