nyt
Silvain Rideau
1091 Evans
silvain.rideau@berkeley.edu
www.normalesup.org/~srideau/eng/teaching

Final (Lecture 003)

May 12th

- To do a later question, you can always assume a previous question.
- There are three problems (the third one is on the other side).
- 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 is true (you do NOT have to prove it):

- *For all prime* $p \geqslant 3$ *and* $k \in \mathbb{Z}_{\geqslant 0}$*, there exists* $n \in \mathbb{Z}$ *such that* $\gcd(n,p) = 1$ *and* $(1+p)^{p^k} = 1 + np^{k+1}$.

Problem 1 :

1. Let K be a field, $F \leqslant K$ be its prime subfield and $\sigma : K \to K$ be a (unitary) ring homomorphism. Show that for all $x \in F$, $\sigma(x) = x$.
2. Assume that K is a characterietic $p > 0$ field. Show that $x \mapsto x^p$ is an injective (unitary) ring endomorphism of K.
3. Using the above, show Fermat's small theorem : for all $x \in \mathbb{Z}$ and $p \in \mathbb{Z}$ prime such that $\gcd(p,x) = 1$,x$^{p-1} \equiv 1 \mod p$.

Problem 2 :

1. Let G be an Abelian group and $x, y \in G$ be elements of order m and n respectively such that $\gcd(m,n) = 1$. Show that $\langle x, y\rangle$ is a cyclic group.
2. Let G be an Abelian group and let $x \in G$ have maximal order n in G, show that the order of every element in G divides n.
3. Let K be a field. Show that there are at most n elements in $K^\star$ whose order divides n.
4. Let K be a field, $G \subseteq K^\star$ a finite subgroup. Show that G is cyclic.
5. Form now on, let $p \geqslant 3$ be prime. Let $\varphi : (\mathbb{Z}/p^k\mathbb{Z})^\star \to (\mathbb{Z}/p\mathbb{Z})^\star$ be the map sending $x \mod p^k$ to $x \mod p$. Show that it is a well defined group homomorphism whose kernel is cyclic of order p^{k-1}.
6. Show that $(\mathbb{Z}/p\mathbb{Z})^\star$ is cyclic of order $p-1$. Conclude that there exists $x \in (\mathbb{Z}/p^k\mathbb{Z})^\star$ of order $p-1$.
7. Show that $(\mathbb{Z}/p^k\mathbb{Z})^\star$ is cyclic of order $p^{k-1}(p-1)$.

8. Let $n \in \mathbb{Z}_{\geqslant 1}$ be relatively prime to 2. Show that $(\mathbb{Z}/n\mathbb{Z})^\star$ is isomorphic to a product of cyclic groups whose orders you shall specify.

Problem 3 :
First some definitions:

- An integral domain R is said to be local if it has a unique maximal ideal $\mathfrak{M}$.
- An integral domain R is said to be a discrete valuation ring if there exists $\pi \in R$ such that every element in $\mathrm{Frac}(R)$ is of the form $u\pi^n$ where $u \in R^\star$ and $n \in \mathbb{Z}$.

1. Let R be a local principal ideal domain, show that any two irreducible elements are associated.
2. Let R be a discrete valuation ring (and π be as in the definition of a discrete valuation ring), show that every non zero ideal of R is of the form (π^n) for some $n \in \mathbb{Z}_{\geqslant 0}$.
3. Let R be an integral domain. Show that the following are equivalent:
   (i) R is a local principal ideal domain;
   (ii) R is a unique factorisation domain whose irreducibles are all associated;
   (iii) R is a discrete valuation ring.
4. Let R be a local integral domain. Show that $\mathfrak{M} = R \smallsetminus R^\star$.