Homework 4
due on Monday, October 16

Solve the following problems.

Problem 1. Let F be a finite field with $q = p^n$ elements. Let a be a generator of the multiplicative group $F^\times$ (we proved that this group is cyclic).

a) Let $\mathbb{F}_p[x] \longrightarrow F$ be the map defined by $f(x) \mapsto f(a)$. Prove that this map is a surjective ring homomorphism whose kernel is a principal ideal generated by some irreducible polynomial $g(x) \in \mathbb{F}_p[x]$. Conclude that F is isomorphic to $\mathbb{F}_p[x]/(g)$ and that the degree of g is n. Conclude that g divides $x^q - x$.

b) Let $h \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. prove that $\mathbb{F}_p[x]/(h)$ is a field with $q = p^n$ elements. Conclude that h divides $x^q - x$. Conclude that h has a root b in F. Conclude that the map $\mathbb{F}_p[x] \longrightarrow F$, $f \mapsto f(b)$ induces an isomorphism of $\mathbb{F}_p[x]/(h)$ and F.

c) Use a) and b) to conclude that any two finite fields with q elements are isomorphic.

d) Let g be as in a). Prove that if b is a root of g then so is b^p. Conclude that $a, a^p, ..., a^{p^{n-1}}$ are distinct roots of g.

e) Let f be an automorphism of the field F. Prove that there is $0 \le k < n$ such that $f(x) = x^{p^k}$. Conclude that the group of all automorphisms of F is cyclic of order n.

f) Let I_n be the set of all monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$. Prove that

$$x^{p^n} - x = \prod_{k|n} \prod_{f \in I_k} f.$$

Let i_n be the cardinality of I_n. Conclude that

$$p^n = \sum_{k|n} k i_k.$$

This allows to compute i_k for every k.

Problem 2. Let K be a field and let R be an integral domain containing K as a subring and finite dimensional as a K-vector space. Prove that R is a field.

Problem 3. Solve problems 3,4 to section 7.2. In addition, prove that when R is a field, then $R[[x]]$ is an Euclidean domain. Consult problem 5 to 7.2. and example 4 in section 8.1.

Problem 4. Ler R be a UFD and let S be a multiplicative subset of R. Prove that $S^{-1}R$ is a UFD. Is the same true with UFD replaced by PID?

Problem 5. Let A be an ordered abelian group (like the integers). A valuation on an integral domain R is a function $v : R - \{0\} \longrightarrow A$ such that

1. $v(ab) = v(a) + v(b)$ for all $a, b \in A$;
2. $v(a + b) \geq \min(v(a), v(b))$ for all $a, b \in A$, such that $a + b \neq 0$

Let v be a valuation on R.

a) Let K be the field of fractions of R. For a non-zero element a/b of K define $v(a/b) = v(a) - v(b)$. Prove that v is well defined and it is a valuation on K.

b) Define a function $w : R[x] - \{0\} \longrightarrow A$ by $w(f) =$ the smallest of the valuations of the non-zero coefficients of the polynomial f. Prove that w is a valuation on $R[x]$.

c) Use b) to prove Gauss' Lemma. Hint: if R is a UFD then any irreducible element of R corresponds to a discrete valuation on R (i.e. the valuation has values in the integers).

Problem 6. Let R be an integral domain with PACC. Prove that $R[x]$ has PACC.

Problem 7. a) Let p be an odd prime and $n \geq 1$ an integer. Prove that if a is an integer such that $a - 1$ is divisible by p but it is not divisible by p^2 then the image of a in the multiplicative group of $\mathbb{Z}/p^n\mathbb{Z}$ is p^{n-1}. Conclude that the multiplicative group of $\mathbb{Z}/p^n\mathbb{Z}$ is cyclic and if a is a primitive root modulo p then either the image of a or the image of $a + p$ generates this group.

b) Let $n \geq 3$. Prove that the order of the image of 5 in the multiplicative group of $\mathbb{Z}/2^n\mathbb{Z}$ is 2^{n-2}. Conclude that the multiplicative group of $\mathbb{Z}/2^n\mathbb{Z}$ is a direct product of a cyclic group of order 2^{n-2} and a cyclic group of order 2.