Homework 3
due on Thursday, October 15

Problem 1. Solve problems 3,4 to section 7.2 in Dummit and Foote. 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 2. Ler R be an integral domain.

a) Let $f, g \in R[x]$ be such that $fg = cx^n$ for some n and some $c \in R$, $c \neq 0$. Prove that there exist elements $a, b \in R$ and $m \leq n$ such that $f = ax^m$ and $g = bx^{n-m}$ and $ab = c$.

b) Suppose that $f = f_0 + f_1 x + ... + f_n x^n \in R[x]$. Suppose that there is a prime ideal P of R such that $f_n \notin P$, $f_0, ..., f_{n-1} \in P$ and $f_0 \notin P^2$. Prove that if $f = gh$ for some $g, h \in R[x]$ then one of g, h is constant. Conclude that if in addition f is monic then it is irreducible in $R[x]$. This result is known as **Eisenstein criterion**. Hint: Assume that $f = gh$ and both g, h have positive degree. Pass to the ring $(R/P)[x]$ and apply a) to show that constant terms of g and h belong to P. Derive contradiction.

c) Prove that the polynomial $2x^{10} + 21x^8 - 35x^2 + 14$ is irreducible in $\mathbb{Z}[x]$. Hint: Apply Eisenstein criterion with appropriate prime ideal P.

Problem 3. 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 4. 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 Kdefine $v(a/b) = v(a) - v(b)$. 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; we discussed it in class).

Problem 5. Let R be an integral domain with PACC. Prove that $R[x]$ has PACC.

Problem 6. Let R be a commutative ring and let $R[x]$ be the ring of polynomials in x with coefficients in R. Let $f = f_0 + f_1 x + ... + f_n x^n \in R[x]$. Prove that

a) f is invertible iff $f_0 \in R^\times$ and $f_1, ..., f_n$ are nilpotent.

b) f is nilpotent iff $f_0, ..., f_n$ are nilpotent.

c) f is a zero divisor iff $af = 0$ for some $0 \neq a \in R$.

d) Let P be a prime ideal of R and $f, g \in R[x]$. Prove that all coefficients of fg belong to P iff either all coefficients of f or all coefficients of g belong to P.

e) If f belongs to every maxiaml ideal of $R[x]$ then f is nilpotent.

Problem 7. 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) Show that there is unique monic irreducible polynomial $g \in \mathbb{F}_p[x]$of degree n such that $g(a) = 0$. 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.

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

c) 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 8. Let R be a commutative ring and S a multiplicative subset of R. For an R module M consider the set $M \times S$ and the relation $(m, s) \sim (n, t)$ iff $r(tm - sn) = 0$ for some $r \in S$.

a) Show that $\sim$ is an equivalence relation. Denote the equivalence class of (m, s) by $\frac{m}{s}$ and the set of all equivalence classes by $S^{-1}M$. Prove that the operation

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st}$$

is well defined and makes $S^{-1}M$ and abelian group.

b) For $\frac{r}{t} \in S^{-1}R$ and $\frac{m}{s} \in S^{-1}M$ define

$$\frac{r}{t}\frac{m}{s} = \frac{rm}{ts}.$$

Prove that this is a well defined operation which makes $S^{-1}M$ into and $S^{-1}R$-module.

c) Let $f : M \longrightarrow N$ be a homomorphism of R-modules. Show that $\hat{f} : S^{-1}M \longrightarrow S^{-1}N$ given by

$$\hat{f}(\frac{m}{s}) = \frac{f(m)}{s}$$

is well defined and it is a homomorphism of $S^{-1}R$-modules.

d) A sequence of R-module homomorphisms $M \xrightarrow{f} N \xrightarrow{g} P$ is **exact** if the kernel of g coincides with the image of f. Prove that if

$$M \xrightarrow{f} N \xrightarrow{g} P$$

is an exact sequence then so is

$$S^{-1}M \xrightarrow{\hat{f}} S^{-1}N \xrightarrow{\hat{g}} S^{-1}P.$$

In particular, if M is a submodule of N then $S^{-1}M$ can be naturally considered as a submodule of $S^{-1}N$.

e) Let N, P be submodules of an R-module M. Prove that

1. $S^{-1}(N+P) = S^{-1}N + S^{-1}P$;
2. $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$;
3. the $S^{-1}R$-modules $S^{-1}(M/N)$ and $S^{-1}M/S^{-1}N$ are isomorphic.

f) For an R-module M define the annihilator of M as

$$ann(M) = \{r \in R : rm = 0 \text{ for all } m \in M\}.$$

Prove that $ann(M)$ is an ideal. Prove that $S^{-1}ann(M) = ann(S^{-1}M)$ provided M is a finitely generated R-module..

g) Let N, P be submodules of an R-module M. Define

$$(N : P) = \{r \in R : rx \in N \text{ for all } x \in P\}.$$

Prove that $(N : P)$ is an ideal in R. Prove that $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$ provided P is finitely generated.