

Homework 3

due on Monday, October 24

Solve problems 17,18 to section 10.3 of Dummit and Foote. In addition 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 $a, a^p, \dots, a^{p^{n-1}}$ are distinct roots of g .

e) Let f be an automorphism of the field F . Prove that there is $0 \leq k < n$ 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 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 $S^{-1}M$ an 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 an $S^{-1}R$ -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

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

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.

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

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

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

f) 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.

Problem 3. For a prime ideal P of a commutative ring R and an R -module M define $M_P = S^{-1}M$, where $S = R - P$. M_P is called the **localization** of M at P . Let $f : M \longrightarrow N$ be a homomorphism of R -modules. Prove that the following are equivalent:

1. f is injective;
2. $\hat{f} : M_P \longrightarrow N_P$ is injective for all prime ideals P ;
3. $\hat{f} : M_P \longrightarrow N_P$ is injective for all maximal ideals P ;

Prove the same with *injective* replaced by *surjective*.