Math 525 Class 12 September 20

New homework is posted. Due Wed 27^{th}.

Friday Sept 22: Quiz on 9.1.

Monday Sept 25: Holiday.

Wed Sept 27: No quiz.

Midterm: End of Ch. 9.

We will not cover "Grobner Bases"

Claim: The proof of the main theorem of Ch. 8, Sec 3 is really an adaptation of the proof that integers factor uniquely into primes.

Let's review that proof:

First define a prime to be a number $p > 1$ such that p has no factors except $1, p$.

(Can also consider ± 1, $\pm p$)

Math 525 — Quiz 06 – September 20, 2023

Name: Solutions

1. Complete the statement the main theorem of Section 8.3: Every Principal Ideal Domain is a . . .

Unique Factorization Domain

2. (This is a "fuzzy" question—try to answer as best you can.) In the proof of the main theorem of Section 8.3, we have to prove that the process of factoring "stops" at some point. How is this proven?

If factoring continues indefinitely, we have an infinite ascending chain of ideals, which is impossible in a PID.

3. Complete the following definition: An nonzero, non-unit element r in an integral domain R is *irreducible* if . . .

$r = ab \Rightarrow$ one of a, b is a unit

4. Complete the following definition: An nonzero, non-unit element r in an integral domain R is *prime* if . . .

Whenever $r \mid ab$ then $r \mid a$ or $r \mid b$

OR: (r) is a prime ideal.

5. Prove that in an integral domain R, a prime element is always irreducible.

Suppose r is prime and r factors as $r = ab$. Then $r \mid a$ or $r \mid b$.

WLOG $r \mid a$, so $a = rx$ and $r = rxb$, so $xb = 1$ and b is a unit.

Thus r is irreducible.

From point of view of 8.3 we defined a prime to be an irred. elt of $\mathbb{Z}$.

Factorization stops because if $n = ab$ $a \neq 1$ $b \neq 1$ then $a < n$ and $b < n$.

There is no infinite descending sequence in $\mathbb{N}$.

This proves that factorizations exist, but not that they are unique.

To prove uniqueness, need Lemma:
If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Std. proof: Assume $p \nmid a$ and show $p \mid b$.
If $p \nmid a$, $\gcd(a,p) = 1$. By ~~Eulere~~ Euclid, $1 = xa + yp$

$b = xab + ypb$, so $p \mid b$.

With Lemma, do an induction.
If $n = p_1^{e_1} \cdots p_m^{e_m} = q_1^{f_1} \cdots q_r^{f_r}$

Use the lemma to remove a p_1 from both sides and reduce to a smaller case.

How do these steps get translated to the proof of 8.3?

We define irreducible (similar) and prime ($p|ab \Rightarrow p|a$ or $p|b$).

Having defined irred. we prove that "factorization stops" at some point.
(This was because PID satisfies ACC.)

Thus we have factorization existence but not uniqueness.

To get the uniqueness, we needed our lemma ~~for~~ $p|ab \Rightarrow p|a$ or $p|b$.

~~Thus~~. In this setting we prove irreducible $\Rightarrow$ prime.
This is Proposition 11, which shows more

Prop 11: irred $\Leftrightarrow$ prime in a PID

and in fact, if p is irred

it is shown that (p) is maximal.

(This is the substitute for the Euclid Lemma.)

Now with the existence of factorizations

and the $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ lemma,

we can do the induction as before.

Note: We do have something approximately

like the ~~Eu~~ Euclidean Algorithm in a

general PID.

Proposition 6: Let R be a PID and

a, b nonzero in R. Let d be a generator

for (a, b). Then

(1) $d = \gcd(a, b)$

(2) $d = xa + yb \quad x, y \in R$.

(3) d is unique up to units.

Note: the proof of Prop. 11 does NOT proceed by analogy with the Euclid Lemma.

The part not on quiz was that.

p irreducible $\Rightarrow$ p prime.

Suppose (m) is an ideal containing (p), where p is irred. Then $p \in (m)$

so $p = xm$ for some x.

p irred $\Rightarrow$ either x unit or m is a unit.

m unit $\Rightarrow$ $(m) = R$.

x unit then $(m) = (p)$.

Thus the only ideal strictly containing (p) is R. and so (p) is maximal and therefore prime.

Q: Can we produce a proof more analogous to the proof for $\mathbb{Z}$ based on proposition 6?