Math 525 October 4 Class 17

Quiz solutions next page.

Remarks on Eisenstein's Criterion

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial which is irreducible. Is it always possible to find a prime p and a substitution $x \longmapsto (x-a)$ such that $f(x-a)$ ~~is~~ and hence f is irred. by Eisenstein?

A: No.

Q: If we wish to use this technique how do we find the a and the p.

A: Luck or experience.

Math 525 — Quiz 9 – October 4, 2023

Name: Solutions

Determine the order and structure of the following abelian groups:

1. $(\mathbb{F}_2[x]/(x^2+x+1))^\times$

Observe that x^2+x+1 is irred. since 1 is not a root and 0 is not a root (Prop 10)
So the quotient is a field. (Prop 15) So the multiplicative group is cyclic. So ans: 3, C_3.

2. $(\mathbb{Z}/8\mathbb{Z})^\times$ Ans: 4, $C_2 \times C_2$ [See Cor. 20]

$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$

Check: $3^2 \equiv 1 \bmod 8$ $5^2 = 25 \equiv 1 \bmod 8$
$7^2 = 49 \equiv 1 \bmod 8$.

3. $(\mathbb{Z}/27\mathbb{Z})^\times$ Ans: 18, C_{18} (See Cor 20)

Exercise: $1+p$ has order p^{n-1} mod p^n.

(We'll think about this later.)

Note also $\mathbb{Z}/27\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z}$

and that $(\mathbb{Z}/3\mathbb{Z})^\times \cong C_2$.

Note also $\left| \left(\mathbb{Z}/p^3\mathbb{Z} \right)^\times \right| = (p-1)p^2$

only div by p^2 not p^3, so

there is no element of order p^3.

Remarks on 9.6 (Mostly Skipped).

You should know the Hilbert Basis Theorem.

it says that If R is Noetherian, then

$R[x]$ is Noetherian.

This means that $F[x_1, \dots, x_n]$ is Noetherian

for any field F, so $\mathbb{C}[x_1, \dots, x_n]$ is Noetherian.

<u>Alg. Geom:</u> An algebraic set is defined by a

finite collection of polynomials.

"Basis" is a misnomer (historically a basis

was a set of generators for an ideal, but

we no longer use the word "basis" this way).

In the proof we consider an ideal

$I \subset R[x]$ and the ideal L

of all leading coeff. of polyns in I

We also consider L_d = all leading coeff

of polyn. of degree d in I (+ 0)

~~Observe that~~ L, and L_d are ideals.

if $a \in L_{d-1}$ then $\exists f = ax^{d-1} + \dots$

so $xf = ax^d + \dots$

so $a \in L_d$. That is

$L_1 \subset L_2 \subset \dots \subset L_d \subset L_{d+1} \subset \dots \subset L$

and this is finite by ACC.

Midterm Fri Oct 13th.