ath 525 Class 19 October 9

Schedule: HW 9.2, 9.3, 9.4 due today

Fixed error 9.4.19(e).

HW 9.5, 9.6 due Wednesday Oct 11.

Midterm Friday Oct 13

I will post blank copies of all quizzes.

WW: Observes that $a^p \equiv a \mod p$.

and $a^{p-1} \equiv 1 \mod p$ if $a \not\equiv 0 \mod p$.

This is NOT necessary for 9.4.19 (d).

Good to know generalization $a^{\varphi(m)} \equiv 1 \mod m$

if $(a, m) = 1$.

Example of a "fuzzier" question:

What does the Hilbert Basis Theorem say?

A: That $R[x]$ is Noetherain if R is.

~~we~~ In the proof of the Hilbert Basis Theorem, we must transfer our knowledge about ideals of R to ideals of $R[x]$.

Why does the ACC for ideals of R imply anything at all about ideals of $R[x]$?

<u>Intended answer</u>: If I is an ideal of $R[x]$, then the set of leading coefficients of polynomials in I (plus zero) is an ideal of R. (This works also with the modifier "of degree d".)

Thus ~~properties~~ we a connection ideals of $R[x]$

$\longrightarrow$ ideals of R and properties can be ~~refl~~ transferred.

What is a likely question for the midterm?

Should be short and have a concrete answer.

Easily computable in a few minutes.

Nice if it uses one or more theorems in boo

What is the order and structure of the group

$$\left[\mathbb{F}_2[x] / (x^3 + x + 1) \right]^\times \; ?$$

Observation 1: $x^3 + x + 1$ is irred in $\mathbb{F}_2[$

because 1 is not a root and 0 is not a root.

Thus $\mathbb{F}_2[x]/(x^3+x+1)$ is a field.

This field is a V.S. of dim 3 over $\mathbb{F}_2$

and has order 8. Thus the units have order

The mult. group of a finite field is cyclic so

the group is isomorphic to C_7.

Similarly: We showed that a Euclidean Domain is a PID. This means that given an ED R and an ideal $I \subset R$, we must produce an $a \in I$ such that $I = (a)$. Where do we get the ~~a~~ a?

A: We choose $a \in I$ to be an ~~the~~ element of smallest nonzero norm. Then show this a works.

Another type of question: State the <X> theorem or fill in the blanks in the statement of <X> theorem.

Give an example to show that the hypothesis <H> of <X> Theorem is necessary.

Or: <X> theorem says $A \Rightarrow B$, is it true that $B \Rightarrow A$? Give a proof or counterexample.

Specific example: We proved that a PID is a UFD. Is it true that UFD $\Rightarrow$ PID? Proof or counterexample.

Counterexamples $\mathbb{Z}[x]$, $\mathbb{R}[x,y]$.

What are ideals in these rings that aren't principal?

How do you know they are UFDs?