Math 525 October 2 Class 16

Quiz solutions next page.

Wed: Quiz on 9.5.

We will (mostly) skip 9.6

Midterm soon! Date negotiable. (Friday 13^{th}).

Math 525 — Quiz 8 – October 2

Name: Solutions

1. Let $\mathbb{F}_2$ be the field with 2 elements and consider the polynomial $p(x) = x^3 + 1 \in \mathbb{F}_2[x]$. Is p irreducible? If so, prove it; if not, give a factorization.

No. p has a root, $1 \in \mathbb{F}_2$

$p(1) = 1^3 + 1 = 1 + 1 = 0.$

Alternative: $(x+1)(x^2+x+1) = x^3 + 1$ in $\mathbb{F}_2[x]$

2. Is the following proposition true or false? Explain your answer.

Proposition: A polynomial $f \in \mathbb{Z}[x]$ has a factor of degree one if and only if f has a root in $\mathbb{Z}$.

False. Let $2x - 1 = f(x)$ then f has a factor of degree 1 but the root $\frac{1}{2} \notin \mathbb{Z}$.

3. What goes in the blanks in the following statement of Eisenstein's Criterion? Put your answers below the proposition.

Proposition (Eisenstein's Criterion) Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial in $R[x]$ $(n \geq 2)$. Suppose that $a_{n-1}, \ldots, a_1, a_0$ __________ and that a_0 __________. Then $f(x)$ __________.

$\in P$

$\notin P^2$

is irreducible in $R[x]$.

4. Show that the polynomial $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$, by substitution of $x + 1$ for x.

(Next page)

Quiz # 4.

x^4+1 is irred. iff $(x+1)^4+1$ is irred.

$$(x+1)^4+1 = x^4+4x^3+6x^2+4x+1+1$$

$$= x^4+4x^3+6x^2+4x+2$$

irred. by Eisenstein with $p=2$.

Why is this polynomial interesting?

x^4+1 is reducible mod p for every prime p.

This will be proved in Ch. 14.

Also elementary proof (no Galois Theory) in Amer. Math. Monthly.

This shows that the argument

"$f(x)$ is irreducible mod p, so

$f(x)$ is irreducible in $\mathbb{Z}[x]$"

More generally what is going on in this section: reduction mod p, Eisenstein etc. are all a bunch of tricks.

These tricks only work in special cases.

If we choose some random polynomial in $\mathbb{Z}[x]$ of degree 12, it's probably irred and probably these tricks won't work to show irreducibility.

There is an algorithm for factoring polyn in $\mathbb{Z}[x]$. Idea find a bound on the possible coefficients of factors and try factors.

Remarks about the results of 9.3.

Gauss' Lemma and

$R[x]$ is a UFD iff R is a UFD.

Gauss Lemma says that if $p(x) \in R[x]$ factors in $F[x]$ (where F is the field of fractions of R) then p factors in $R[x]$.

Q: How does the proof use R being a UFD?

A: In a UFD ~~irr~~ a irred. in R implies a prime. (i.e. (a) is a prime ideal of R.)

This means that $R/(a)$ is an integral domain so $R/(a)[x]$ is also an integral domain. So if we have in $R[x]$

$f(x)g(x) = a\,h(x)$.

reducing mod (a) we get

$\bar{f}(x)\bar{g}(x) = 0$ in $R/(a)[x]$

and so either $\bar{f}(x)$ or $\bar{g}(x)$ is zero in $R/(a)[x]$.

This says we can take the factorization in $F[x]$, clear denominators, so

$d\,p(x) = a(x)\,b(x)$ in $R[x]$

and start eliminating irred. factors of d.

Q: How does the proof that $R[x]$ is a UFD iff R is work?

A: Gauss' Lemma says that factorization in $R[x]$ and $F[x]$ is "the same". $F[x]$ is a UFD because it's Euclidean.

Example: $\mathbb{Z}[2i]$ is NOT a UFD because the field of fractions is $\mathbb{Q}[i]$, and in $\mathbb{Q}[i][x]$ $x^2+1 = (x+i)(x-i)$ but in $\mathbb{Z}[2i][x]$ x^2+1 is irreducible.