Notes

November 14, 2014

#10

$\mathbb{Q}[x]/\langle x^2+2\rangle \cong \mathbb{Q}[x]/\langle x^2+1\rangle$

no, can't find $\beta \in \mathbb{Q}[x]/\langle x^2+2\rangle$ where $\beta = -[2]$

note that if we replace $\mathbb{Q}$ with $\mathbb{R}$ then we get an isomorphism.

is $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ a field?

is $x^2+x+1 \in \mathbb{Z}_2[x]$ irreducible?

$[0],[1]$ are not roots and degree is ≤ 3 and so it is a field.

question

if $f(x) \in \mathbb{Z}_p[x]$ where p is prime and $f(x)$ is irreducible. how many elements does $\mathbb{Z}_p/f(x)$ have? $\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} : a_i \in \mathbb{Z}_p\}$ and so p^n elements.

#24

you can always find such an $f(x)$ (of any degree).

thm

assume $f(x) = g(x)h(x)$ where $f(x) \in \mathbb{Z}[x]$ and $h(x), g(x) \in \mathbb{Q}[x]$. then we can factor $f(x)$ into poly with integer coefficients of the same degree.

proof

$g(x) \in \mathbb{Q}[x]$ with $g(x) = \frac{1}{b}g_1(x)$ where $g_1(x) \in \mathbb{Z}[x]$ and $b \in \mathbb{Z}$ and $g(x) = \frac{c}{b}g_2(x)$ where $g_2(x) \in \mathbb{Z}[x]$ and $b, c \in \mathbb{Z}$ and $g_2(x)$ is a primitive polynomial

say $\gcd(m,n) = 1$

$f(x) = \frac{m}{n} \cdot \frac{s}{t} g_2(x)h_2(x)$.

multiplying two primitive polynomials gives a primitive polynomial

thm

eisenstein's irreducibility criterion)

corollary 4.4.7