Test 2 Corrections: ① Redo any questions completely where points are missed — on separate paper.
② Explain mistakes made on original test
If these are correct, get $\frac{1}{2}$ pts back.
Return/complete before Nov 15

More about polynomials & Fields

From last time

Fact: If p is a prime, then
$\frac{x^p - 1}{x-1}$ is irreducible in $\mathbb{Z}[x]$.

FYI - this is called the p^{th} cyclotomic polynomial.

Pf. $\frac{x^p-1}{x-1} = 1+x+x^2+\dots+x^{p-1} = p(x)$
(Because $(x-1)(x^{p-1}+x^{p-2}+\dots+x+1) = x^p - 1$.)

Consider $p(x+1) = 1+(x+1)+(x+1)^2+\dots+(x+1)^{p-1}$

$$= \frac{(x+1)^p - 1}{(x+1)-1} = \frac{x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \dots + \binom{p}{p-1}x + 1 - 1}{x}$$

$$= x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-1}$$

This fits the Eisenstein criterion $p \mid$ each coeff. except first.

$p^2 \nmid p$ = constant term.

$\therefore$ By Eisenstein $p(x+1)$ is irreducible.

If $p(x)$ were reducible, $p(x) = r(x)s(x)$ for some poly. of deg ≥ 1, in $\mathbb{Z}[x]$, and then we would have $p(x+1) = r(x+1)s(x+1)$, which would mean $p(x+1)$ is reducible also. $\times$. $\therefore p(x)$ is irred. $\blacksquare$

eg $x^6+x^5+x^4+x^3+x^2+x+1$ is irreducible over $\mathbb{Q}$.

Question: Is $x^5+x^4+x^3+x^2+x+1$ irreducible?

No! $x=-1$ is a zero! $x^5+x^4+x^3+x^2+x+1$

$=(x+1)(x^4+x^2+1)$.

Let R be a commutative ring with unity.
Let I be an ideal in R. A basis for I is a subset $\{b_1,\dots,b_k\}$ such that $I=\langle b_1,b_2,\dots,b_k\rangle$.

Hilbert basis theorem. Every ideal in $\mathbb{F}[x_1,\dots,x_k]$ has a finite basis.

field

---

eg $R=\mathbb{Q}[x,y]$ is $\mathbb{Q}[x][y]$ is a UFD

$x^2y+\frac{2}{3}x^5y^2-2$

$I=\langle\{x^k-y^m$, where k & m are even positive integers$\}\rangle=\langle p_1(x,y),\dots,p_n(x,y)\rangle$

$I=\langle\{f(x,y)\in\mathbb{Q}[x,y]:$ $f(x,y)$ vanishes on no more than 10 integer points$\}\rangle$

We say the field E is an extension field of the field F if $F\leq E$.

subring that is a subfield.

Given a field F & extension field E and an element $\alpha \in E$, we define the evaluation homomorphism

$$\phi_\alpha : F[x] \to E \text{ by } \phi_\alpha(f(x)) = f(\alpha) \in E.$$

for all $f(x) \in F[x]$.

Note $F \subseteq F[x]$ (the constant polynomials),

and $\phi_\alpha(a) = a$ for all $a \in F$. $g(x) = a$

$$\phi_\alpha(\underset{x}{1 \cdot x}) = \alpha$$

Example: $\alpha = 0 \Rightarrow \phi_0(f(x)) = a_0$, where

$$f(x) = a_0 + a_1 x + \cdots + a_k x^k.$$

Kronecker's Theorem. Let F be a field, $f(x)$ a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an element $\alpha \in E$ such that $f(\alpha) = 0$.

Pf. Since $F[x]$ is a UFD, $f(x)$ must have an irreducible factor $p(x)$. Then $\langle p(x) \rangle$ is maximal, so $E = F[x]/\langle p(x) \rangle$ is a field. Let

$\psi : F \to E$ be defined by $\psi(a) = a + \langle p(x) \rangle$.

Note this is 1-1: If $\psi(a) = \psi(b) \Rightarrow a + \langle p(x) \rangle = b + \langle p(x) \rangle$

$\Rightarrow a - b \in \langle p(x) \rangle \Rightarrow a - b = c(x)p(x) \Rightarrow c(x) = 0$

degree ≥ 1 — for some $c(x) \in F[x]$

$a - b = 0 \Rightarrow a = b. \therefore \psi$ is 1-1.

$\Rightarrow F \cong \underset{\text{subfield}}{\psi(F)} \subseteq E.$

Set $\alpha = x + \langle p(x) \rangle \in E$, not in $\psi(F)$.

Observe that $\phi_\alpha(p(x)) = p(\alpha) = p(x + \langle p(x) \rangle)$

Let $p(x) = a_0 + a_1 x + \dots + a_k x^k$

$$p(x + \langle p(x) \rangle) = a_0 + a_1(x + \langle p(x) \rangle) + a_2(x + \langle p(x) \rangle)^2 + \dots + a_k(x + \langle p(x) \rangle)^k$$

Note $(x + \langle p(x) \rangle)^j = x^j + (\text{stuff}) \langle p(x) \rangle$
$= x^j + \langle p(x) \rangle.$

$$\Rightarrow p(x + \langle p(x) \rangle) = \underbrace{a_0 + a_1 x + \dots + a_k x^k}_{p(x)} + \langle p(x) \rangle$$
$$= \langle p(x) \rangle = 0.$$

$\therefore p(\alpha) = 0.$ $\boxtimes$

$\mathbb{Q}[x]/\langle x^2 - 2 \rangle \longrightarrow$ A field where $\sqrt{2}$ exists

$\mathbb{R}[x]/\langle x^2 + 1 \rangle \rightsquigarrow$ A field where $\sqrt{-1}$ exists.

$\mathbb{R}[x]/\langle x^2 - 2 \rangle$ not a field.
$\uparrow$ reducible

Defn: An element $\alpha \in E$, where $F \leq E$ is <u>algebraic over F</u> if $\exists\, p(x) \in F[x]$ s.t. $p(\alpha) = 0$ in E.

α is called transcendental over F if no such polynomial exists.

eg $\sqrt{2}$ is alg. over $\mathbb{Q}$.

π, e are transc. over $\mathbb{Q}$.
