3/2
Monday
week 7

Chapter 9 continued...

Ex: Is $f(x) = x^3 - 3x - 1$ irreducible or reducible over $\mathbb{Q}$?

Since $\deg(f) = 3$, then f is reducible iff f has a root in $\mathbb{Q}$.

By the rational roots thm, if $f(\frac{r}{s}) = 0$ then $r \mid (-1)$ and $s \mid 1$.

Rational roots thm

$f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$
If $f(\frac{r}{s}) = 0$ where $\frac{r}{s} \in \mathbb{Q}$ and $\gcd(r,s) = 1$ then
$r \mid a_0$ and $s \mid a_n$

So, $r = \pm 1$, $s = \pm 1$.

Possible roots are $\frac{r}{s} = 1, -1$.

And

$$f(1) = 1^3 - 3(1) - 1 = -3 \neq 0$$

$$f(-1) = (-1)^3 - 3(-1) - 1 = 1 \neq 0.$$

So, f has no roots/zeros in $\mathbb{Q}$.

Since $\deg(f) = 3$, f is irreducible over $\mathbb{Q}$

Prop (Eisenstein's Criterion)

Let p be a prime,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x],$$

$a_n \not\equiv 0 \pmod{p}$

$a_i \equiv 0 \pmod{p}$ for $0 \leq i < n$

and $a_0 \not\equiv 0 \pmod{p^2}$.

$p \nmid a_n$
$p \mid a_i \quad 0 \leq i < n$
$p^2 \nmid a_0$

Then $f(x)$ is irreducible over $\mathbb{Q}$.

proof: In book. ▨

Ex: Show that $x^4 + 10x + 5$ is irreducible over $\mathbb{Q}$.

Let $p = 5$.

$p \nmid 1$

$p \mid 10$, $p \mid 5$

$p^2 \nmid 5$

So, $x^4 + 10x + 5$ is irreducible.

Prop: Let F be a field.

The maximal ideals of $F[x]$ are the ideals $(f(x))$ where $f(x) \in F[x]$ is irreducible in $F[x]$.

In particular, $F[x]/(f(x))$ is a field iff $f(x)$ is irreducible over F.

Pf: Since $F[x]$ is a PID all of its ideals are principal.

Note that $(0) = \{0\}$ is not maximal, since $(0) \subseteq (x) \subseteq F[x]$ and $(x) \neq F[x]$ and $(0) \neq (x)$.

Let $f(x)$ be a nonzero poly in $F[x]$.

Then, $(f(x))$ is maximal
iff $(f(x))$ is a prime ideal } since $F[x]$ is a PID and $(f(x)) \neq (0)$.
iff $f(x)$ is irreducible over F. } since $F[x]$ is a PID

∎

Vector spaces

Def: A set V is said to be a vector space over a field F if

① V is an abelian group under some binary operation $+$

and for each $\alpha \in F$ and $v \in V$ there exists an element $\alpha v \in V$ such that the following

(i) If $v, w \in V$, then $v+w \in V$
(ii) If $v, w, z \in V$ then $(v+w)+z = v+(w+z)$
(iii) $\exists\, 0 \in V$ where $0+v = v+0 = v$ for all $v \in V$
(iv) If $v \in V$, there exists a unique vector with $v+(-v) = (-v)+v = 0$. $-v \in V$
(v) $v+w = w+v$ for all $v, w \in V$

Conditions hold for all $\alpha, \beta \in F$ and $v, w \in V$:

② $\alpha(v+w) = \alpha v + \alpha w$

③ $(\alpha+\beta)v = \alpha v + \beta v$

④ $\alpha(\beta v) = (\alpha\beta)v$

④ $1v = v$

Ex:

II

V :

$+\alpha w$

$+\beta v$

$)v$

Ex: $V = \mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{R}\}$

is a vector space over $F = \mathbb{R}$.

addition of vectors

$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$

scalar mult.

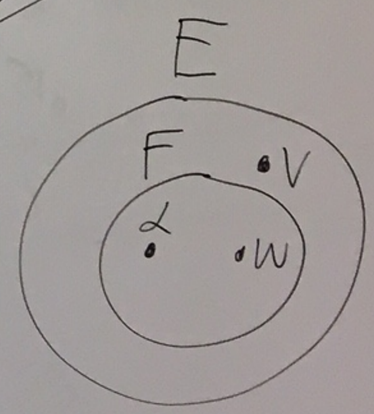
$\alpha(a_1, a_2, \ldots, a_n) = (\alpha a_1, \alpha a_2, \ldots, \alpha a_n)$

Ex: Let E be a field and F be a subfield of E.

E is a vector space over F. Here, $V = E$, $F = F$.

$v + w \leftarrow$ field addition

$\alpha v \leftarrow$ field multiplication



Ex: $V = \mathbb{C} = \{ a + ib \mid a, b \in \mathbb{R} \}$

$F = \mathbb{R}$

Then $\mathbb{C}$ is a vector space over $\mathbb{R}$.

vector addition

$(a+ib) + (c+id) = (a+c) + i(b+d)$

scalar mult. $[\alpha \in F = \mathbb{R}]$

$\alpha(a+ib) = \alpha a + i\alpha b$

Def: Let V be a vector space over a field F.
Let $v_1, v_2, \dots, v_n \in V$.

① The span of $v_1, v_2, \dots, v_n$ is $\operatorname{span}(\{v_1, v_2, \dots, v_n\}) = \{ \underbrace{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n}_{\text{linear combination of } v_1, v_2, \dots, v_n} \mid \alpha_1, \alpha_2, \dots, \alpha_n \in F \}$.

We say $v_1, v_2, \dots, v_n$ span V if
$V = \operatorname{span}(\{v_1, v_2, \dots, v_n\})$.

② We say that $v_1, v_2, \dots, v_n$ are linearly dependent if there exist $\alpha_1, \alpha_2, \dots, \alpha_n \in F$, not all zero, with $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$. Otherwise we say $v_1, v_2, \dots, v_n$ are linearly independent.

Another way to say linearly independent: $v_1, v_2, \dots, v_n$ are linearly independent if the only solution to $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$ is $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$

(3) We say that $v_1, v_2, \dots, v_n$ is a <u>basis</u> for V if $v_1, v_2, \dots, v_n$ span V and $v_1, v_2, \dots, v_n$ are linearly independent.

<u>Ex:</u> $V = \mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$

$F = \mathbb{R}$

<u>Claim:</u> $v_1 = 1$, $v_2 = i$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.

(1) $\text{span}(\{1, i\}) = \{\alpha_1 \cdot 1 + \alpha_2 \cdot i \mid \alpha_1, \alpha_2 \in \mathbb{R}\} = \{\alpha_1 + \alpha_2 i \mid \alpha_1, \alpha_2 \in \mathbb{R}\} = \mathbb{C}$

So, $1, i$ span $\mathbb{C}$.

(2) $1, i$ are linearly independent over $\mathbb{R}$.

Suppose

$$\alpha_1 1 + \alpha_2 i = 0$$

where $\alpha_1, \alpha_2 \in \mathbb{R}$.

If $\alpha_2 \neq 0$, then $i = -\frac{\alpha_1}{\alpha_2} \in \mathbb{R}$.

But $i \notin \mathbb{R}$.

So, $\alpha_2 = 0$.

So,

$$\alpha_1 1 = 0.$$

Thus,

$$\alpha_1 = 0.$$

Thus, $\alpha_1 = \alpha_2 = 0$ is the only solution to $\alpha_1 1 + \alpha_2 i = 0$ where $\alpha_1, \alpha_2 \in \mathbb{R}$.

By (1) and (2), $\beta = \{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.