4/7

next Tuesday

- Reminder April 14^{th} – Exam 2.

I will post a review of topics later today. on webpage

WORK on it & we can talk about on Thurs.

Ex 2

- won't cover rings.

- 16^{th}, 21^{st}, 23^{st} ← review for final.

---

little bit of ring theory, then some group theory.

Def. R comm ring w/ 1.

~~the~~ Let $a, b \in R$. We say a divides b if $\exists\, k \in R$ s.t. $ak = b$.

---

aR principal ideal gen'd by a.

$= \{x \mid \exists\, r \in R \;\; x = ar\}$

a divides b iff $b \in aR$.

$\mathbb{Z}$ $\quad 6 \mid 12 \quad 12 \in 6\mathbb{Z}$.

Thm TFAE

1) R is a field
2) $R[x]$ is a Euclidean domain
3) $R[x]$ is a PID.

Eucl Domain - is a domain w/ a Norm N where you can do a division algorithm.

$\Rightarrow$: R field the degree function is always a norm but you get a division algorithm

$\forall\, f(x), g(x)\ (g(x) \neq 0)\ \exists\, q(x), r(x)$

$f(x) = \cancel{q(x)g(x)}\ q(x)g(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

$\mathbb{Z}[x]$

$f(x) = x^2 + 3x + 1$

$g(x) = \cancel{2x}\, x + 1$

$$
\begin{array}{r|l}
 & x + 2 \\
\hline
x+1 & x^2 + 3x + 1 \\
 & -x^2 + x \\
\hline
 & \cancel{2x + 2} \\
 & 2x + 1 \\
 & -2x + 2 \\
\hline
 & -1
\end{array}
$$

$x^2 + 3x + 1 = (x+1)(x+2) - 1$

③ $f(x) = x^2 + 3x + 1$

$g(x) = 2x + 1$

$$2x+1 \overline{\big) \, x^2 + 3x + 1} \quad \frac{1}{2}x$$

$\frac{1}{2}x \notin \mathbb{Z}[x]$

$R[x]$ is a PID. WTS R is a field.

$a \in R$, $a \neq 0$ need to show $\exists\, x \in R$ $ax = 1$

$I = aR[x] + xR[x]$. By hypothesis

$aR[x] + xR[x] = d(x)R[x]$

$d(x) = d_0 + d_1 x + \dots + d_n x^n$ $a \in$ so a

$a = d(x) \cdot u(x)$ $\deg(a) = 0$

$\deg(d(x)u(x)) = \deg(d(x)) + \deg(u(x))$

So $\deg(d(x)) = 0$ $d(x) = d_0$.

$\deg(u(x)) = 0$ $u(x) = u_0$. $a = d_0 \cdot u_0$

$x \in d(x)R[x]$ $x = d_0 \cdot v(x)$ $\deg v(x) = 1$

$v(x) = v_1 x$ $d_0(v_1 x) = x$

$d_0 v_1 = 1$ so d_0 is a unit

(4) we use the other part

$$d(x) = d_0 \in aR[x] + xR[x]$$

$$d_0 = a \cdot k(x) + x \cdot j(x)$$

$$d_0 = a(k_0 + k_1 x + \dots + k_n x^n) + x(j_0 + j_1 x + \dots + j_m x^m)$$

$$= ak_0 + ak_1 x + \dots + ak_n x^n$$
$$\cancel{j_0 x + \dots + j_i x + \dots} + j_m x^{m+1}$$

$$d_0 = ak_0$$

$$\underline{1 = d_0^{-1} d_0 = a(d_0^{-1} k_0)} \Rightarrow a \text{ is } \underline{\text{a unit}}$$

Observe

$aR[x] + xR[x]$ being principal $\Rightarrow$ a is a unit.

So in $\mathbb{Z}[x]$ give me an idea that is not principal.

$\underline{2\mathbb{Z}[x] + xR[x] \text{ is not principal}}$

(5)

If F is a field

ex. $\mathbb{R}$, $\mathbb{C}$.

$\mathbb{Z}_n$ (n prime)

$\mathbb{Q}$.

Given $f(x) = f_0 + f_1 x + \dots + f_n x^n$ $(f_n \neq 0)$

$\mathbb{Q}(\sqrt{2})$
$= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
field

Prop $\alpha \in F$ is a root of $f(x)$ iff $(x-\alpha) \mid f(x)$.

(Need to know Proof for final)

$(a+b\sqrt{2})(c+d\sqrt{2})$
$= (ac + 2bd) + (ad+bc)\sqrt{2}$

Pf.

$\Rightarrow$ α is a root.

$F[x]$ is a Eucl. dom w/ deg( ) as its norm. why?. b/c F field.

$\mathbb{Q}(\sqrt[3]{2})$

$a + b\sqrt[3]{2} + c\sqrt[3]{4}$

$\mathbb{Q}(i)$

$\{a + bi \mid a, b \in \mathbb{Q}$

Let $g(x) = x - \alpha$. Choose $g(x), r(x)$

$f(x) = g(x)(x-\alpha) + r(x)$.

and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.
$(\deg r(x) = 0)$

α a root

$0 = f(\alpha) = g(x)(\alpha - \alpha) + r(\alpha)$. $= r(\alpha) = r_0 = r(x)$

So $f(x) = g(x)(x-\alpha)$. So $(x-\alpha) \mid f(x)$

$\Leftarrow$ If $(x-\alpha) \mid f(x)$ $\exists\, g(x)$ $f(x) = (x-\alpha) g(x)$

$f(\alpha) = (\alpha - \alpha) g(\alpha) = 0$. $\therefore \alpha$ is a root.

(6) D a domain

$D \times (D \setminus \{0\})$

(a, b) $b \neq 0$.

$$(a,b) = \frac{a}{b} = \frac{c}{d}$$

$(a,b) \sim (c,d)$ iff $da - bc = 0$

the set of equiv classes is a field

$$\frac{a}{b} := [(a,b)]$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ab+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

$R[x]$

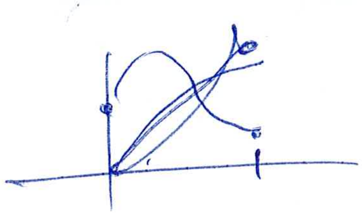
$\downarrow$

$R(x)$ the field of rational function.

<u>group hom.</u> $\varphi : G \to H$ $(G, \cdot), (H, \Delta)$

$\forall g_1, g_2$ $\varphi(g_1 g_2) = \varphi(g_1) \Delta \varphi(g_2)$

<u>Ex</u> take $C([0,1])$ - group under + of cont functions.



$\varphi : C([0,1]) \to \mathbb{R}$

$\varphi(f(x)) = \int_0^1 f(x)dx$

$\varphi(f(x)+g(x))$
$= \int (f(x)+g(x))dx$
$= \int f(x)dx + \int g(x)d$
$= \varphi(f) + \varphi(g)$

⑦ $\psi_1(f(x)) = \int_0^{1/2} f(x)\,dx.$

$$\psi(x) = \int_0^1 x\,dx = \frac{x^2}{2}\Big|_0^1 = 1/2$$

$$\psi_1(x) = \int_0^{1/2} x\,dx \quad \frac{x^2}{2}\Big|_0^{1/2} = \frac{1}{8}$$

$$\phi(f(x)) = \int_0^1 f(x)^2\,dx$$

$$\phi(f(x)+g(x)) = \int_0^1 (f(x)+g(x))^2\,dx$$

$$= \int_0^1 f(x)^2\,dx + \int_0^1 2f(x)g(x)\,dx + \int_0^1 g(x)^2\,dx$$

$$= \phi(f(x)) \qquad \phi(g(x))$$

$$\int_0^\infty f(t)\,e^{-st}\,dt \quad ??? \quad \text{Laplace}$$

8

$n > 1$

$\mathbb{Z}_n$

$1 \leq j < n$

$\varphi_j : \mathbb{Z}_n \to \mathbb{Z}_n$

$\varphi(1) = j$

$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1)$
$= j + j = 2j$

$\varphi_j(k) = kj$

real-definitn

$\varphi_j(k + n\mathbb{Z}) = kj + n\mathbb{Z}$.

φ_j is a group homomorphism.

$\forall k_1, k_2 \in \mathbb{Z}_n$ $\varphi_j(k_1 + k_2) = j(k_1 + k_2) = jk_1 + jk_2 = \varphi_j(k_1) + \varphi_j(k_2)$

?? when is φ_j an isom. iff φ_j is a bijection.

$f : A \to A$ A finite. TFAE 1) f is bijection
2) f is injective
3) f is surjective.

φ_j is an isom iff φ_j is injective.

Aside

(9) S $\varphi : G \to H$ is a gp hom.

φ is inj iff $\operatorname{Ker}\varphi = \{e_G\}$

Pf. $\Rightarrow$ φ is inj. Let $x \in \operatorname{Ker}\varphi$.

$\varphi(x) = e_H = \varphi(e_G)$ inj. $\Rightarrow$ $x = e_G$.

So $\operatorname{Ker}\varphi = \{e_G\}$.

$\Leftarrow$ S $\operatorname{Ker}\varphi = \{e_G\}$.

$\varphi(g_1) = \varphi(g_2)$ $\qquad$ $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H$

$\varphi(g_1)\varphi(g_2)^{-1} = e_H$

$g_1 g_2^{-1} \in \operatorname{Ker}\varphi = \{e_G\}$

$g_1 g_2^{-1} = e_G$

$g_1 = g_2$. So φ is inj

1st Isom Theorem $\qquad$ $\varphi : G \to H$ gp hom.

1) $\varphi(G) \le H$.

2) $\operatorname{Ker}\varphi \trianglelefteq G$.

$\bar{\varphi} : G/\operatorname{Ker}\varphi \to \varphi(G)$ $\qquad$ 3) $G/\operatorname{Ker}\varphi \cong \varphi(G)$

$\bar{\varphi}(g\operatorname{Ker}\varphi) = \varphi(g)$

$g_1\operatorname{Ker}\varphi = g_2\operatorname{Ker}\varphi$. $\quad$ $\varphi(g_2^{-1}g_1) = e_H$ $\quad$ $\varphi(g_1) = \varphi(g_2)$

$g_2^{-1}g_1 \in \operatorname{Ker}\varphi$

10

W.D. $\quad f: \cancel{A} \to B$

if $a_1 = a_2$, then $f(a_1) = f(a_2)$

Inj if $f(a_1) = f(a_2)$ then $a_1 = a_2$

$\varphi_j : \mathbb{Z}_n \to \mathbb{Z}_n$

$\varphi_j(k) = jk$ $\qquad \varphi_j$ isom?

φ_j is inj.

$\operatorname{Ker} \varphi_j = \{k \mid jk = 0\}$

$= \{k \mid n \mid jk\}$.

$\operatorname{Ker} \varphi_2$

$\varphi_2 : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$. $\quad \{k \mid 10 \mid (2k)\} = \{0, 5\} = \langle 5 \rangle$

$0 \leq j < n$.

φ_j inj ~~Ker~~ 0 the only

$\{k \mid n \mid jk\}$

$\varphi_3 : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ $\qquad \{k \mid 10 \mid 3k$ $\;$ k is a multiple of 10 $\}$

$k = 0$

(11) $\varphi_j : \mathbb{Z}_n \to \mathbb{Z}_n$.

Prove (later) φ_j is a isom iff $\gcd(j,n)=1$

φ_j is an isom

φ_j is a bijection

φ_j is an injection φ

φ_j is a surjection

φ_j is an automorphism

$\gcd(j,n)=1$

$\varphi_3 : \mathbb{Z}_7 \to \mathbb{Z}_7$ $\varphi_3 \in Aut(\mathbb{Z}_7)$

what is its order

$\varphi_3 \circ \varphi_3 \circ \varphi_3$

$\varphi_3, \varphi_3^2, \varphi_3^3, \dots, Id.$