Subrings

A subring S of a ring R is a subset $S \subseteq R$ s.t. S is also a ring with the operations on R.

Proposition 16.10. *Let R be a ring and S a subset of R. Then S is a subring of R if and only if the following conditions are satisfied.*

1. $S \neq \emptyset$.
2. $rs \in S$ for all $r, s \in S$.
3. $r - s \in S$ for all $r, s \in S$.

] $\Leftarrow$ $gh^{-1} \in S$ when $g, h \in S \Leftrightarrow S$ a subgroup of R

Ex] R = 2×2 real matrices

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\} \quad \text{is a subring}$$

- Non-empty
- $A \cdot B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}$
- $A - B \in T$, $A, B \in T$.

More on Integral Domains and Feilds

commutative division Ring $\Leftrightarrow$ $\forall r \neq 0 \; \exists r^{-1}$ (↑ mult. inverse)

Commutative ring without zero div.

Gaussian Integers

Ex] $\mathbb{Z}[i] = \{ m + ni \mid m, n \in \mathbb{Z} \}$. This is a ring

Also an integral domain.

an element in a ring with a mult. inverse.

Show $\mathbb{Z}[i]$ is not a feild by finding all units

Suppose $\alpha = a + ib$ is a unit with mult. inverse $\beta = c + id$

If $\alpha\beta = 1$ we know $|=\overline{1}$ — complex conjugate

$$\Rightarrow \quad \overline{\alpha\beta} = \alpha\beta$$

$$\overline{\alpha}\,\overline{\beta} = \alpha\beta = 1$$

$$1 = \alpha\beta\overline{\alpha}\,\overline{\beta} = (a+ib)(c+id)(a-ib)(c-id)$$

$$= (a^2+b^2)(c^2+d^2)$$

$$\Rightarrow \quad (a^2+b^2) = (c^2+d^2) = \pm 1$$

$\therefore$ either $a+ib = \pm 1$ or $a+ib = \pm i$.

$\therefore$ the only units are $\pm 1, \pm i$ $\therefore$ $\mathbb{Z}[i]$ is not a field.

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

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} .$$

Prop (cancelation Law):

Let D be a comutive ring with $1 \in D$. Then D is integral iff $\forall a \in D$ $a \neq 0$ whenever $ab = ac$ $b = c$.

Proof: First suppose D is an integral domain.

Let $ab = ac$, $a \neq 0$

since no zero divisor ← iff $fg = 0 \Rightarrow$ either $f = 0$ or $g = 0$.

$$ab - ac = 0 \Rightarrow a(b-c) = 0$$

$$\Rightarrow b - c = 0 \Rightarrow b = c$$

Suppose cancellation holds in D

Let $ab = 0$ (say $a \neq 0$)

$a0 = 0$

So $ab = a0 \Rightarrow b = 0$

$\therefore$ $\exists$ no zero divisors.

■.

Theorem: Every finite integral domain is a feild.

Proof: Let D be a finite integral domain.

$D^* =$ non-zero elements in D

Define a map $\lambda_a : D^* \to D^*$ for each $a \in D^*$

$d \mapsto da$

Note this is okay if $a \neq 0$ and $d \neq 0$ $\Rightarrow ad \neq 0$ Since D is an integral domain

λ_a is 1-1 : If $\lambda_a(d_1) = \lambda_a(d_2)$

$\Rightarrow ad_1 = ad_2 \Rightarrow d_1 = d_2$ (By cancelation)

λ_a is onto because D^* is a finite set an λ_a is 1-1

$\exists\ d \in D^*$ s.t. $\lambda_a(d) = ad = 1$ and $\lambda_a : D^* \to D^*$

$\therefore$ d is a left inverse of a

But since D is an integral domain it is commutative

$\therefore ad = da = 1$ $\therefore a^{-1} = d$.

$\therefore$ D is a feild.

■

if $a'd = ad = 1$

$\lambda_a(d) = \lambda_{a'}(d)$

$a'd - ad = 0$

$(a' - a)d = 0$

Def Let $n \geq 0$ $n \in \mathbb{Z}$, $r \in R$ a ring

write $nr = \underbrace{r + \cdots + r}_{n \text{ times}}$

The <u>characteristic</u> of R is

$\text{Char}(R) =$ least positive $n \in \mathbb{Z}$ s.t. $nr = 0$ $\forall r \in R$

$= 0$ if no such n exists.

Ex $\text{char}(\mathbb{Z}_p) = p$ for p prime. $\mathbb{Z}_p$ is a feild since every non-zero element has an inverse.

$\forall a \in \mathbb{Z}_p \quad pa = 0$

$\text{Char}(\mathbb{R}) = \text{Char}(\mathbb{C}) = \text{Char}(\mathbb{Q}) = 0$

Lemma Let R be a ring, $1 \in R$. $|1| = n$ (mult. order) then $\text{char}(R) = n$. If $n1 \neq 0$ $\forall n \neq 0$ $\text{Char}(R) = 0$

Proof: Say $n < \infty$ $n \cdot 1 = 0$. Fix $r \in R$

$nr = n(1r) = (n1)r = 0r = 0$

if $n = \infty$ then $\text{char}(R) = 0$

∎