3/28/11

Def: R is called an <u>integral domain</u> if R is commutative and R contains no zero divisors.

<u>Examples</u>

1) $R = \mathbb{Z}$

2) $R = \mathbb{Z}[x] = \{$polynomials with integer coefficients$\}$

How come there are no zero divisors for $\mathbb{Z}[x]$?

Take $p(x), q(x) \in \mathbb{Z}[x]$, $p(x) \neq 0 \neq q(x)$.

Can write $p(x) = \sum_{i=0}^{n} \alpha_i x^i$ $\quad q(x) = \sum_{j=0}^{m} \beta_j x^j$

Suppose s is the minimal power of x in $p(x) \ni \alpha_s \neq 0$. Similarly, suppose t is the minimal power of x in $q(x) \ni \beta_t \neq 0$

$p(x) \cdot q(x) = \Sigma\,(\text{garbage}) + \alpha_s \beta_t x^{s+t}$

nothing in (garbage) can cancel $\alpha_s \beta_t x^{s+t}$ since all powers involved are strictly larger than $s+t$.

<u>ex:</u> $p(x) = x^3 + x + 1$, $\quad q(x) = -1000x^5 - 25$

$s = t = 0$

$p(x) \cdot q(x) = -25 + \Sigma\,(\text{garbage})$

Def: $x \in R$, $x \neq 0$ is called a <u>unit</u> if R is unital and $\exists\ y \in R$ with $xy = yx = 1_R$

Terminology: $R^{\times} = \{$units in R$\}$

<u>Examples</u>

1) $R = \mathbb{Z}$, $\quad \mathbb{Z}^{\times} = \{1, -1\}$

2) $R = \mathbb{Z}_n$, $\quad (\mathbb{Z}_n)^{\times} = U(n) = \{m \in \mathbb{Z}_n : \gcd(m,n) = 1\}$

If $x \in \mathbb{Z}_n$, $x \notin U(n)$ then $\gcd(x,n) \neq 1$, so $\exists$ an element $y \in \mathbb{Z}_n$ with $xy = n \pmod{n} = 0$, then $x \notin U(n) \Rightarrow x \notin$ (

Suppose $x \in U(n)$. Then by Euclidean algorithm,
$\exists$ $k, l \in \mathbb{Z}$ with $xk + ln = 1$
Reduce mod n,

$$\begin{aligned} 1 &= (xk + ln) \pmod n \\ &= (xk) \bmod n + \underbrace{(ln) \bmod n}_{=0} \\ &= xk \bmod n \\ &= x \cdot (k \bmod n) \end{aligned}$$

so $k \bmod n$ is the inverse of x. Hence $x \in (\mathbb{Z}n)^\times$

Def: Let R be a ring with unit 1_R. Then R is called a <u>division ring</u> if every nonzero $x \in R$ belongs to $R^\times$.

Examples
1) $R = \mathbb{R}$
2) $R = \mathbb{Q}$
3) $R = \mathbb{C}$

$\}$ these are all commutative though...

Example of a noncommutative division ring:
4) $R \subseteq M_2(\mathbb{C})$

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

$R = \{ aI + bj + ck + di \ : \ a, b, c, d \in \mathbb{R} \}$

$$\begin{aligned} aI + bj + ck + di &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} + \begin{pmatrix} 0 & ci \\ ci & 0 \end{pmatrix} + \begin{pmatrix} di & 0 \\ 0 & -di \end{pmatrix} \\ &= \begin{pmatrix} a+di & b+ci \\ ci-b & a-di \end{pmatrix} \end{aligned}$$

determinant: $(a+di)(a-di) - (b+ci)(ci-b)$
$= a^2 + d^2 + b^2 + c^2$

det is zero iff $a = b = c = d = 0$, that is if you have the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
Hence, R is a division ring.
noncommutative since $ij \neq ji$.

Def: A commutative division ring is called a **field**.

Examples
1) $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are all fields
2) $\mathbb{Z}_p$ is a field $\forall$ primes p.

Prop: Let R be a ring with unit 1_R. Then if $x \in R$, x a zero divisor implies x is not a unit, conversely, if x is a unit then x is not a zero divisor

Pf: $\Rightarrow$ Suppose x is a zero divisor. Then $x \neq 0$ and $\exists$ $y \in R$, $y \neq 0$, with $xy = 0$. If x had an inverse z, then

$z(xy) = z \cdot 0 = 0$

But, $(zx)y = z(xy)$

$(zx)y = 1_R \cdot y = y$

Hence $y = 0$. contradiction. $\therefore$ x can't be a unit

$\Leftarrow$ Suppose x is a unit. Then $\exists$ $z \in R$, $zx = xz = 1_R$

Suppose there is $y \in R$, $y \neq 0$, $xy = 0$

Since $z \cdot x = 1_R$, multiply by y on the right to obtain $(zx)y = 1_R \cdot y = y$

$(zx)y = z(xy) = z \cdot 0 = 0$

Then $y = 0$, contradiction.

Hence x is not a zero divisor ∎

Def: Let R be an integral domain (commutative, no zero divisors) Then R is a Euclidean Domain if $\exists$ $d: R \to \mathbb{N} \cup \{0\}$ with

1) $d(a) \leq d(ab)$ $\forall$ $a, b \in R$, $b \neq 0$
2) $\forall$ $a, b \in R$, $b \neq 0$ $\exists$ $q, r \in R$ with $a = bq + r$ and either $r = 0$ or $d(r) < d(b)$ (d = division algorithm)

Examples

1) $R = \mathbb{Z}$, $d(n) = |n|$

2) $R = \mathbb{F}[x]$ where $\mathbb{F}$ is a field
$\mathbb{F}[x] = \{$polynomials with coefficients in $\mathbb{F}\}$

You have polynomial division
$d(p) = \text{degree}(p)$