Section 19 - Integral Domains

Key property of numbers: $xy = 0 \Rightarrow x = 0$ or $y = 0$.

If x, y are elements of some ring R, this can fail:

In $\mathbb{Z}_6$, have $2 \neq 0 \neq 3$, but

$$(2)(3) = 0.$$

This complicates solving polynomial equations, e.g. to solve equation

$$x^2 + x = 0 \qquad x \in R,$$

for some ring R, try

$$x^2 + x = x(x+1) = 0.$$

If $R = \mathbb{Q}$, conclude $x = 0$ or $x + 1 = 0$ ($\Leftrightarrow x = -1$).

In general more solutions exist, e.g. for $\mathbb{Z}_6$ have solutions

$$x = 0, \quad x = -1 \ (= 5), \quad x = 2, \quad x = 3.$$

Def Let R be a ring, $a_s \in R \setminus \{0\}$. If there is a $b \in R \setminus \{0\}$ s.t.

$$ab = 0 \quad \text{or} \quad ba = 0,$$

say a is a **0-divisor**.

Example In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, there are no 0-divisors.

- In $\mathbb{Z}_6$, the 0-divisors are $2, 3, 4$, since

$$(2)(3) = (4)(3) = 0,$$

$$(1)b = b \neq 0 \text{ if } b \neq 0$$

$$(5)b = -b \neq 0 \text{ if } b \neq 0.$$

Thm In $\mathbb{Z}_n = \{0, \ldots, n-1\}$, $m \in \mathbb{Z}_n$ is a 0-divisor if and only if $\gcd(m, n) \neq 1$.

Proof $a^m, b^k \in \mathbb{Z}_n$ satisfies $a^m b^k = 0$ $\Leftrightarrow$ mk divisible by n.

If $d = \gcd(m, n) > 1$, let $k = \frac{n}{d}$, so

$$mk = m\frac{n}{d} = \frac{m}{d} n, = 0 \quad \text{in } \mathbb{Z}_n,$$

so m is 0-divisor.

If $\gcd(m, n) = 1$, then for $k \in \mathbb{Z}$, n divides $mk \iff n$ divides k.

Hence $mk = 0$ in $\mathbb{Z}_n \iff k = 0$ in $\mathbb{Z}_n$,

so m is not a 0-divisor.

Corollary Let p be a prime. Then $\mathbb{Z}_p$ has no 0-divisors.

Proof $0 < m \leq p - 1 \Rightarrow \gcd(m, p) = 1$.

Cancellation laws

A ring R satisfies cancellation laws if for all $a, b, c \in R$, $a \neq 0$

$$ab = ac \Rightarrow b = c$$

and $$ba = ca \Rightarrow b = c.$$

Thm R has cancellation laws $\iff$ R has no 0-divisors.

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

$$\overset{\text{"no 0-divisors"}}{\Longrightarrow} b - c = 0 \Rightarrow b = c$$

□

Integral domains ("helområde")

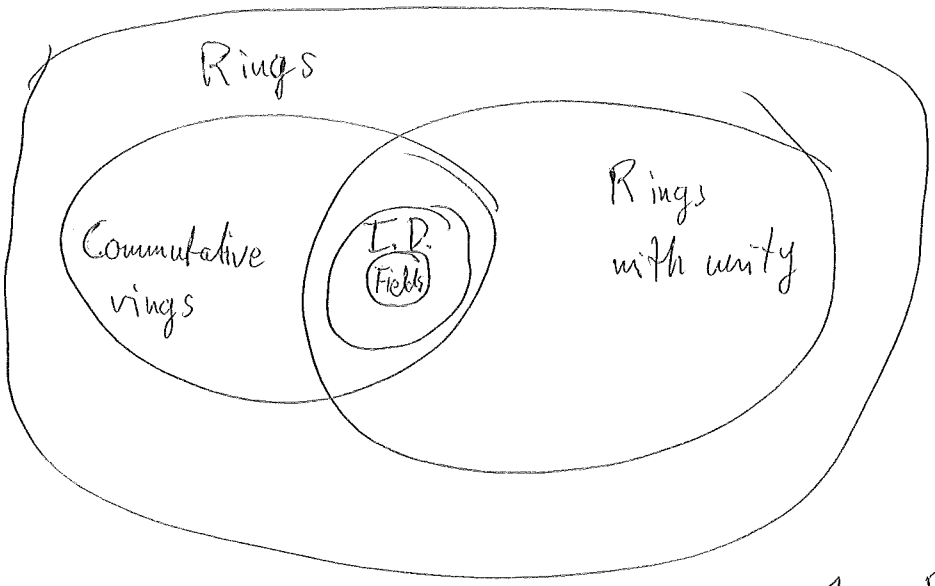
Def A ring D is an integral domain if it has unity, is commutative, and has no 0-divisors.

Example • $\mathbb{Z}$, $\mathbb{Z}_p$ are integral domains.

• Every field F is an integral domain: Let $a, b \in F$, $a \neq 0$

$$ab = 0 \Rightarrow a^{-1}ab = a^{-1}0 \Rightarrow b = 0,$$

so a is not a 0-divisor.



Thm Let R be a finite integral domain. Then R is a field.

Proof Let $R = \{0, 1, a_1, \ldots a_n\}$. Must show for $i = 1, \ldots n$ that a_i is a unit (= has multiplicative inverse).

Consider $a_i 0, a_i 1, a_i a_1, \ldots, a_i a_n$. (*)

By cancellation law, these are distinct, $a_i a_j = a_i a_k \Rightarrow a_j = a_k$.

Hence every element of R is found once in among (*).

In particular, there is a j s.t. $a_i a_j = 1$. □

Corollary $\mathbb{Z}_p$ is a field if p is prime.

Notational remark: In an integral domain D, if $a \in D$ is a unit, $b \in D$, write $\frac{b}{a}$ for $a^{-1}b = ba^{-1}$.

Usual fraction rules apply:

$$\frac{a}{1} = a, \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}, \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Characteristic of a ring: Let R be a ring. If there exists an $n \in \mathbb{Z}^+$ s.t. $n \cdot a = 0$ for all $a \in R$, then smallest such n is characteristic of R.

If no such n exists, R has <u>characteristic 0</u>.

<u>Thm</u> If R has unity, then characteristic is either

- smallest $n>0$ s.t. $n \cdot 1 = 0$, or
- 0 if no $n>0$ exists with $n \cdot 1 = 0$.

Fermat's (little) theorem

Spot the pattern a^k in $\mathbb{Z}_n$

$\mathbb{Z}_2$	k: 0	1
a: 0	0	0
1	1	1

$\mathbb{Z}_3$	1	2
0	0	0
1	1	1
2	2	1

$\mathbb{Z}_4$	1	2	3
0	0	0	0
1	1	1	1
2	2	0	0
3	3	1	3

$\mathbb{Z}_5$	1	2	3	4
0	0	0	0	0
1	1	1	1	1
2	2	4	3	1
3	3	4	2	1
4	4	1	4	1

$\mathbb{Z}_7$	1	2	3	4	5	6
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

Thm (Fermat's little theorem) If p is a prime and $0 \neq a \in \mathbb{Z}_p$, then $a^{p-1} = 1$.

Equivalently: If p is a prime, $a \in \mathbb{Z}$ s.t. p does not divide a, then p divides $a^{p-1} - 1$.

Proof: In any ring R (with unity), the units form a group under multiplication.

$\mathbb{Z}_p$ is a field $\Rightarrow$ Units are $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

In finite group G, $a^{|G|} = e$ for all $a \in G$. (from Lagrange's thm)

In $\mathbb{Z}_p^*$, $a^{|\mathbb{Z}_p^*|} = a^{p-1} = 1$.

□

Corollary: Let p be a prime, $a \in \mathbb{Z}$. Then p divides $a^p - a$.

Proof $a^p - a = a(a^{p-1} - 1)$. If p does not divide a, it divides $a^{p-1} - 1$.

Example 11 does not divide $2^{11213} - 1$.

Proof $2^{11213} = 2^{11210}\, 2^3 = (2^{11210})^{10} 2^3 \equiv 2^3 \pmod{11}$.

$2^{11213} - 1 \equiv 2^3 - 1 \not\equiv 7 \not\equiv 0 \pmod{11}$.

Euler's theorem (generalising Fermat)

Thm Let $n \in \mathbb{Z}^+$. The non-0-divisors in $\mathbb{Z}_n$ form a group under multiplication.

Proof: Let $G_n = \{ a \in \mathbb{Z}_n \mid a \text{ is not a 0-divisor} \}$

1. G_n closed under multiplication.

   Assume for contradiction $a, b \in G_n$, $ab \notin G_n$.

   Then have $c \neq 0$ such that

   $$abc = 0$$
   $$\Rightarrow \quad a(bc) = 0$$
   $$\xRightarrow{a \in G_n} \quad bc = 0$$
   $$\xRightarrow{b \in G_n} \quad c = 0, \quad \text{contradiction.}$$

2. G_n a group. Identity, associativity ok

   Inverses: $G_n = \{1, a_1, \ldots, a_k\}$. For any j, all elements

   $$a_j 1, a_j a_1, \ldots, a_j a_k$$

   are distinct, since

$$a_j a_i = a_j a_k$$

$$\Longrightarrow \quad a_j(a_i - a_k) = 0$$

$$\overset{a_j \in G_n}{\Longrightarrow} \quad a_i - a_k = 0$$

$$\Longrightarrow \quad a_i = a_k.$$

Since there are $|G_n|$ elements $a_j, a_j a_1, \ldots, a_j a_k$, must have some i such that $a_j a_i = 1$. □

Non-0-divisors in $\mathbb{Z}_n$ are $0 \leq k < n$ such that

$$\gcd(k, n) = 1.$$

Euler φ-function, $\varphi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$

$\varphi(n)$ = number of positive $k \leq n$ s.t. $\gcd(k, n) = 1$.

$\varphi(1) = 1$, $\varphi(p) = p - 1$ for p prime.

Euler's theorem: Let $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ s.t. $\gcd(a, n) = 1$.

Then $a^{\varphi(n)} - 1$ is divisible by n.

Proof $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ gives $\phi(a) = b \in \mathbb{Z}_n$.

$\gcd(a, n) = 1 \Longrightarrow b$ is non-0-divisor $(b \in G_n)$

$$\Rightarrow b^{|G_n|} = b^{\varphi(n)} = 1,$$

$$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}.$$