Ring and Field

Definition (Field)

A field F, sometimes denoted by $(F, +, \times)$, is a set of elements with two binary operations, say addition and multiplication (note that these operations may be any binary operations), such that for all $a, b, c \in F$, the following axioms are obeyed:

- $(F, +, \times)$ is an *integral domain*, that is,
  - **(A1-M4)** hold
  - **(M5) Multiplicative identity:** $\forall a \in F$, $\exists 1 \in F$ such that $1a = a1 = a$, 1 is called the multiplicative identity in F.
  - **(M6) No zero divisors:** If $a, b \in F$ and $ab = 0$, then either $a = 0$ or $b = 0$.
- **(M7) Multiplicative inverse:** For each $a \in F$, except 0, there is an element a^{-1} in F such that $aa^{-1} = a^{-1}a = 1$.

Ring and Field

Example

The set of real numbers is a field under addition and multiplication.

Example

Let Q denote the set of rational numbers, that is, $Q = \{\frac{a}{b} |\ a, b$ are reals, with $b \neq 0$ and $\gcd(a, b) = 1\}$. Then, $(Q, +, \times)$ is a field.

Example

Let C be the set of complex numbers. Then, $(C, +, \times)$ is also a field.

Example

The set Z of integers is NOT a field. Note that not every element of Z has a multiplicative inverse; in fact, only the elements 1 and -1 have the multiplicative inverses in the integers.

Ring and Field

Problem: Consider the addition and multiplication arithmetic modulo 8 in the finite set $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Construct the following composition table (addition modulo 8):

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

The additive identity is 0.

Ring and Field

Construct the following composition table (multiplication modulo 8):

$\times_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Ring and Field

Construct the following table of additive and multiplicative inverses:

w	$-w$	w^{-1}
0	0	–
1	7	1
2	6	–
3	5	3
4	4	–
5	3	5
6	2	–
7	1	7

- $-w$ is the additive inverse of w
- w^{-1} is the multiplicative inverse of w
- Z_8 **is NOT a field (only a commutative ring with identity 1)**

Ring and Field

Theorem

Let $Z_n = \{0, 1, 2, \ldots, n-1\}$.

- *(i)* $\langle Z_n, +_n, \cdot_n \rangle$ *is a ring, for all* $n \in N$.
- *(ii)* $\langle Z_n, +_n, \cdot_n \rangle$ *has a multiplicative identity* 1.
- *(iii)* $\langle Z_n, +_n, \cdot_n \rangle$ *is an integral domain.*

Ring and Field

Theorem

Let $Z_n = \{0, 1, 2, \ldots, n-1\}$*. Then,*
$\langle Z_n, +_n, ._n \rangle$ *is a field if and only if* n *is prime.*

Remark: $\langle Z_p, +_p, ._p \rangle$ is known as **Galois field** or finite field, when p is a prime.
It is defined as $GF(p) = \langle Z_p, +_p, ._p \rangle$; p being a prime.

Finding greatest common divisor (gcd)

Definition

Given two integers a and b, the greatest common divisor (gcd) of a and b is $d = \gcd(a, b)$ if the following conditions are satisfied:

1. $d|a$ and $d|b$
2. Any divisor c of a and b is also a divisor of d.

We have:

$$\begin{aligned}
\gcd(a, 0) &= a \\
\gcd(0, 0) &= \textit{undefined} \\
\gcd(a, -b) &= \gcd(-a, b) = \gcd(-a, -b) = \gcd(|a|, |b|)
\end{aligned}$$

Euclid's GCD Algorithm

Given integers $b, c > 0$, we make a repeated application of division algorithms to obtain a series of equations which yield $\gcd(b, c)$:

$$\begin{aligned}
b &= q_1 c + r_1, 0 \leq r_1 < c \\
c &= q_2 r_1 + r_2, 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, 0 \leq r_3 < r_2 \\
\vdots &= \vdots \\
r_{j-2} &= q_j r_{j-1} + r_j, 0 \leq r_j < r_{j-1} \\
r_{j-1} &= q_{j+1} r_j + \boxed{0}
\end{aligned}$$

It is worth noticing that

$$0 \leq r_j < r_{j-1} < r_{j-2} < \cdots < r_2 < r_1 < c$$

Therefore,

$$\gcd(b, c) = \gcd(c, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{j-1}, r_j) = r_j.$$

Euclid's GCD Algorithm

Algorithm: EUCLID(b, c)

To compute $\gcd(b, c)$

1: Initialize: $A \leftarrow b$; $B \leftarrow c$
2: **if** $B = 0$ **then**
3: **return** $A = \gcd(b, c)$
4: **end if**
5: Compute $R \leftarrow A \bmod B$
6: Set $A \leftarrow B$
7: Set $B \leftarrow R$
8: goto Step 2

Complexity: If j is the total number of iterations or steps needed to compute $\gcd(b, c)$, then $j < \lfloor 3.\log_e(c) \rfloor$, where $c = \min\{b, c\}$.

Problem: Compute $\gcd(1970, 1066)$.

Using the Euclid's gcd algorithm, we have the following computations:

$$
\begin{aligned}
1970 &= 1 \times 1066 + 904 \\
1066 &= 1 \times 904 + 162 \\
904 &= 5 \times 162 + 94 \\
162 &= 1 \times 94 + 68 \\
94 &= 1 \times 68 + 26 \\
68 &= 2 \times 26 + 16 \\
26 &= 1 \times 16 + 10 \\
16 &= 1 \times 10 + 6 \\
10 &= 1 \times 6 + 4 \\
6 &= 1 \times 4 + 2 \\
4 &= 2 \times \boxed{2} + 0
\end{aligned}
$$

Therefore, $\gcd(1970, 1066) = 2$.
We see that $j =$ number of iterations needed to compute $\gcd(1970, 1066)$ $= 11$ and $j < \lfloor 3.\log_e(c) \rfloor = \lfloor 3.\log_e(1066) \rfloor = 20$

Finding greatest common divisor (gcd)

Lemma

If $d = \gcd(a, b)$, then there exist integers x and y such that $d = ax + by$, where x and y are called the multipliers of a and b, respectively.

Problem: Find the multipliers x, y and z such that $\gcd(170, 128, 217) = 170x + 128y + 217z$.
Solution: We know,

$$\gcd(170, 128, 217) = \gcd[\gcd(170, 128), 217]. \quad (1)$$

To compute $\gcd(170, 128)$, we proceed as follows:

$$\begin{aligned} 170 &= 1 \times 128 + 42 && (2) \\ 128 &= 3 \times 42 + 2 && (3) \\ 42 &= 21 \times 2 + 0. \end{aligned}$$

Finding greatest common divisor (gcd)

Therefore, we have:

$$\begin{aligned} 2 &= \gcd(170, 128) \\ &= 128 - 3 \times 42, \text{ using Eqn (3)} \\ &= 128 - 3 \times [170 - 1 \times 128] \text{ using Eqn (2)} \\ &= (-3) \times 170 + 4 \times 128. \end{aligned} \tag{4}$$

Now, to compute $\gcd(2, 217)$, we proceed as follows:

$$\begin{aligned} 217 &= 108 \times 2 + 1 \qquad (5) \\ 2 &= 2 \times 1 + 0. \end{aligned}$$

Finding greatest common divisor (gcd)

Then,

$$\begin{aligned}
1 &= \gcd(2, 217) \\
&= \gcd[\gcd(170, 128), 217] \\
&= \gcd(170, 128, 217) \\
&= 217 - 108 \times 2, \text{using Eqn (5)} \\
&= 217 - 108 \times [(-3) \times 170 + 4 \times 128], \text{using Eqn (4)} \\
&= 324 \times 170 + (-432) \times 128 + 1 \times 217.
\end{aligned}$$

Hence, we have: $x = 324, y = -432, z = 1$.

Finding the multiplicative inverse in $GF(p)$

If $\gcd(m, b) = 1$, then b has a multiplicative inverse modulo n. In other words, for positive integer $b < m$, there exists $b^{-1} < m$ such that $b.b^{-1} = 1 \pmod{m}$, where 1 is the multiplicative identity in $GF(p)$.

Algorithm: EXTENDED EUCLID(m, b)

1: Initialize: $(A1, A2, A3) \leftarrow (1, 0, m)$ and $(B1, B2, B3) \leftarrow (0, 1, b)$
2: **if** $B3 = 0$ **then**
3:     **return** $A3 = \gcd(m, b)$; no inverse
4: **end if**
5: **if** $B3 = 1$ **then**
6:     **return** $B3 = \gcd(m, b)$; $B2 = b^{-1} \pmod{m}$
7: **end if**
8: Set $Q = \lfloor \frac{A3}{B3} \rfloor$, quotient when $A3$ is divided by $B3$
9: Set $(T1, T2, T3) \leftarrow (A1 - Q.B1, A2 - Q.B2, A3 - Q.B3)$
10: Set $(A1, A2, A3) \leftarrow (B1, B2, B3)$
11: Set $(B1, B2, B3) \leftarrow (T1, T2, T3)$
12: goto Step 2

Ring and Field

Problem: Find the multiplicative inverse of 550 in $GF(1759)$.

Here, $m = 1759$ and $b = 550$. We need to find $b^{-1} \pmod{m}$, i.e., $550^{-1} \pmod{1759}$.
Applying the extended Euclid's gcd algorithm, we have the following table.

Q	$A1$	$A2$	$A3$	$B1$	$B2$	$B3$	$T1$	$T2$	$T3$
–	1	0	1759	0	1	550	–	–	–
3	0	1	550	1	-3	109	1	-3	109
5	1	-3	109	-5	16	5	-5	16	5
21	-5	16	5	106	-339	4	106	-339	4
1	106	-339	4	-111	355	$\boxed{1}$	-111	355	1

Since $B3 = 1$, so $\gcd(m, b) = B3 = 1$ and multiplicative inverse will be $b^{-1} \pmod{m} = B2 = 355$.
Verification: $b.b^{-1} \pmod{m} = 550.355 \pmod{1759} = 1$.

Ring and Field

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Definition (Irreducible Polynomial)

A polynomial $f(x)$ of degree $n > 0$ over the field K is *irreducible* over K if and only if there do not exist polynomials $g(x)$ and $h(x)$ of degree > 0 over K such that

$$f(x) = g(x).h(x),$$

where multiplication is ordinary polynomial multiplication with coefficients operations in K.

- In other words, a polynomial $f(x)$ is said to be irreducible if it can not be factored into non-trivial polynomials over the same field K. 1 and $f(x)$ are trivial factors of $f(x)$.
- A polynomial $f(x)$ is irreducible over K if and only if there does not exist a polynomial $d(x)$, $0 < deg.d(x) < deg.f(x)$, where $deg.f(x)$ means the degree of the polynomial $f(x)$, such that $d(x)|f(x)$ over K.

Ring and Field

Problem: Determine which of the following are reducible over the Galois (finite) field $GF(2)$:

1. $f(x) = x^4 + 1$
2. $f(x) = x^3 + x + 1$
3. $f(x) = x^3 + 1$
4. $f(x) = x^3 + x^2 + 1$