Example (evaluation homomorphism)**.** Let $R = \{f : \mathbb{R} \to \mathbb{R}\}$ with pointwise addition and multiplication. Let $a \in \mathbb{R}$, define $\phi_a : R \to \mathbb{R}$ and $\phi_a(f(x)) = f(a)$. This is a ring homomorphism.

$$\phi_a(f(x) + g(x)) = (f + g)(a) = f(a) + g(a) = \phi_a(f(x)) + \phi_a(g(x))$$

By pointwise addition. Similarly,

$$\phi_a(f(x)g(x)) = fg(a) = f(a)g(a) = \phi_a(f(x))\phi_a(g(x)).$$

Suppose $a = 2$, so $\phi_2 : f(x) \mapsto f(2)$.

Definition

$\phi : R \to S$ is a homomorphism of rings. Then

$$\ker \phi = \{r \in R : \phi(r) = 0\}.$$

and

$$\operatorname{im} \phi = \{s \in S : \phi(r) = s \text{ for some } r\}.$$

Note. Direct product of rings follows intuitively from that of groups. The projection map is again a homomorphism.

Definition: unit

Let R be a ring with identity. A **unit** in R is an element with a multiplicative inverse.

Example. In $\mathbb{Z}_{12}$, 7 is a unit because $7 \times 7 = 1 \mod 12$. The units are $\{1, 5, 7, 11\}$, coprimes of 12.

In $\mathbb{Z}_7$, 3 is a unit. $3 \times 5 = 1 \mod 7$.

In $\mathbb{Z}$, the units are $\{1, -1\}$. Warning: the answer to "what are the units" is usually not ± 1. This is true for $\mathbb{Z}$.

In $\mathbb{Q}$, the units are all NONZERO elements.

Note. 0 is NEVER a unit. Because by Theorem 18.8, $u0 = 0u = 0 \neq 1$ by definition of multiplicative identity.

Theorem

The units, $U(R)$ of R, form a group under multiplication.

Proof

(i) closure: If u and v are units, so is uv. The inverse of uv is $v^{-1}u^{-1}$.

(ii) associativity: definition of $\times_R$.

(iii) identity: I_R is a unit. It is its own inverse.

(iv) inverses: If u is a unit, so is u^{-1}.

$\square$

Definition: division ring

A **division ring** is one in which every nonzero element is a unit.

Definition: fields

A **field** is a commutative division ring.

Example. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$.

Example (division ring not field)**.** $\mathbb{H}$ real quaternions. They are like complex numbers but worse. Complex numbers are a vector space of dimension 2 over the reals. Quaternions are dimensional 4, $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ with basis $\{1, i, j, k\}$, where $i^2 = j^2 = k^2 = -1$. This is not commutative, similar to cross-product. The inverse comes from conjugation.

What is the additive order of 1_R? We know distributivity laws might be involved.

Example. Let F be a field, and let 1_F be the multiplicative identity. Could 1_F have additive order 6?

No. Suppose $1_F + 1_F + 1_F + 1_F + 1_F + 1_F = 0_F \Rightarrow (1_F + 1_F) \times (1_F + 1_F + 1_F) = 0_F$. In a field, if $xy = 0$, then $x = 0$ or $y = 0$.

Proof

Suppose $x \neq 0$, we will show that $y = 0$. This implies x has a multiplicative inverse, x^{-1}. Then

$$\begin{aligned} xy &= 0 \\ x^{-1}(xy) &= x^{-1}0 = 0 \\ (x^{-1}x)y &= 0 \\ 1_R y &= 0 \\ y &= 0 \end{aligned}$$

$\square$

Therefore, $1_F + 1F = 0$ or $1_F + 1_F + 1_F = 0$. So we found a smaller number for the order!

Definition: characteristic of a field

Let n be the additive order of 1_F. If n finite, the characteristic of F is n. If n is infinite, the characteristic of F is 0.

Theorem

The characteristic of a field is either 0 or a prime.

Example. Extreme example: $\mathbb{Z}_2$ is field.

Example (zero divisors)**.** In $M_2(\mathbb{R})$. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} (0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ In $\mathbb{Z}_{10}, 4 \times 5 = 0$.

Definition: zero divisors

Let R be a ring and $x, y \in R$. If $xy = 0$ but $x \neq 0$ and $y \neq 0$, we call x, y **zero divisors.**

Definition: integral domain

An **integral domain** is a commutative ring with identity that has no zero divisors.

Example. $\mathbb{Z}$.

Example (unrelated)**.** $\mathbb{H}$. Then $\{1, -1, i, -i, j, -j, k, -k\}$ under $\times$ form a group. Then the order of its elements are:

$$\begin{aligned}
1 :& 1 \\
-1 :& 2 \\
i :& 4 \\
-i :& 4 \\
j :& 4 \\
-j :& 4 \\
k :& 4 \\
-k :& 4
\end{aligned}$$

But for D_4, the reflections have order 2, and rotations have order $1, 4, 2, 4$. Element order is a structural property. Q_8 is not abelian, but every subgroup is normal.

So the complete list of groups of order 8 is: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_8, D_4, Q_8$.

Example (complete list of groups with order 1 to 15)**.** Note that prime orders only have $\mathbb{Z}_p$. Orders of p^2 only has $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.

$$\begin{aligned}
1 :& \{e\} \\
2 :& \mathbb{Z}_2 \\
3 :& \mathbb{Z}_3 \\
4 :& \mathbb{Z}_4, V_4 \\
5 :& \mathbb{Z}_5 \\
6 :& \mathbb{Z}_6, S_3 \simeq D_3 \\
7 :& \mathbb{Z}_7 \\
8 :& \text{ described above} \\
9 :& \mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3 \\
10 :& \mathbb{Z}_{10}, D_5 \\
11 :& \mathbb{Z}_{11} \\
12 :& \mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6, D_6, A_4, T \\
13 :& \mathbb{Z}_{13} \\
14 :& \mathbb{Z}_{14}, D_7 \\
15 :& \mathbb{Z}_{15}
\end{aligned}$$