Rings

Our favorite rings for error-correcting codes will be $\mathbb{Z}_2$ or $\mathbb{Z}_p$, $p$ prime or any finite field.

Other favorites are $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ integers, reals, complex #s, rational #s.

By definition, a ring is an abelian group under $+$ with an associative multiplication satisfying left $+$ right distributive laws. See Gallian, Ch. 12, 1st page.

Multiplication need not be commutative. If it is, we say the ring is commutative. Also the ring need not have an identity for multiplication. If it does we say it's a ring with unity or identity and call the identity $1$.

Check Gallian, Examples 1-7 (after defn. of ring).

Example of a non-commutative ring (= Gallian Ex. 4)

$M_2(\mathbb{Z}) = \{ (a \ b) \ | \ a, b, c, d \in \mathbb{Z} \}$

Define

$M_2(\mathbb{Z}) = \{ (a \ b) \ | \ a, b, c, d \in \mathbb{Z} \}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$

This is usual matrix multiplication.
Example of a Ring without unity \( \mathbb{Z} = \{ \text{integers} \} \) (Gallian Ex. 5) with usual + and x

Properties of Rings \( A, b, c \in R = \text{ring} \\
\text{Here we use facts from Gallian Chapter 2} \\
1. \( a \cdot 0 = 0, a = 0 \) \\
2. \( a(-b) = (-a)b = -ab \) where \( b + (-b) = 0 \) \\
3. \( (-a)(-b) = ab \) \\
4. \( a(b-c) = ab - ac \) \\
5. If \( R \) has unity \( 1 \), then \( (-1)a = -a \), \((-1)(-1) = 1 \)

\[ \text{ Pf } \]

1. \( 0 + a \cdot 0 = a(0) = a(0 + 0) = a \cdot 0 + a \cdot 0 \) \\
   \( \Rightarrow 0 = a \cdot 0 \) (by cancellation law for +) \\
   (i.e., subtract \( a \cdot 0 \) from both sides) \\

2. \( a(-b) + ab = a(-b + b) = a \cdot 0 = 0 \) \\
   \( a(-a)(b) + ab = (a + a)b = 0 \cdot b = 0 \) \\

3. \( (-a)(-b) = (-a \cdot (-b)) = (-(-ab)) = ab \) \\
   \( \text{as } -(-x) = x \text{ since } x + (-x) = 0 \) \\

4. \( a(b-c) = a \cdot b + a(-c) = ab - ac \) \\
   \( \uparrow \text{using (2)} \) \\

5. \( \text{ See Homework #2 } \)

Defn. \( S \subseteq R \) is a subring means \( S \) is a ring using the operations \( \circ \) of \( R \).

Subring Test. A non-empty \( S \subseteq R \) is a subring iff \( S \) is closed under subtraction \( \circ \) multiplication.

\[ \text{ Pf. } \]

1. Step subgp test \( \Rightarrow S \) is subgp under + \\
   \( \Rightarrow \) it is abelian under + as \( R \) is \\

\( R \) is assoc., \( \circ \) has 2 distrib. laws \\
\( S \) closed under \( \circ \) \( \Rightarrow S = \text{subring of } R \)
Check the Examples 8–13 in Gallian are subrings. This is in homework #2.

**Example A**  
$\{0\}$ is a subring of $\mathbb{R}$  
Finite subring test applies:  
$0 + 0 = 0 + 0 = 0$  
$0 + 0 = 0$ why?  
(Rule for Mult. #1)

**Example B**  
$S = \{0, 3, 6, 9\}$ is a subring of $\mathbb{Z}_{12}$  
Use finite subring test.  
$S = \{3x | x \in \mathbb{Z}_{12}\}$  
$3x - 3y = 3(x - y) \in S$  
$(3x)(3y) = 9xy \in S$

**Example C**  
$n\mathbb{Z}$ is a subring of $\mathbb{Z}$

**Example D**  
$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ = complex numbers.  
Here $i = \sqrt{-1}$, $i^2 = -1$  
You need to use finite subring test  
$(a + bi) - (c + di) = (a - c) + (b - d)i$  
$a, b, c, d \in \mathbb{Z} \Rightarrow a - c \in \mathbb{Z} \land b - d \in \mathbb{C}$
\[(a+bi)(c+di) = (ac-bd) + i(ad+bc)\]
\[a,b,c,d \in \mathbb{Z} \Rightarrow ac-bcd \text{ and } ad+bc \in \mathbb{Z}\]

Suppose \( R \) is a commutative ring with unity 1, identity for \( \times \).

**Defn. Units in a ring** \( R = U(R) = \{a \in R \mid a^{-1} \in R \} \) such that \( a \cdot a^{-1} = a^{-1} \cdot a = 1 \).

**Claim** \( U(R) \) is a group under \( \times \).

**Proof.** We need to check 4 things:

1. **Closed under \( \times \)**
   
   \[a, b \in U(R) \iff a^{-1}, b^{-1} \in R \]
   
   \[\Rightarrow (ab)^{-1} = b^{-1}a^{-1} \in R \Rightarrow ab \in U(R)\]

2. **Associative law** (true in \( R \)).

3. **1 \in U(R) as 1 = 1^{-1}**

4. **Inverses stay in U(R)**
   
   \[ae \in U(R) \iff a^{-1} \in R \iff (a^{-1})^{-1} = a \in R\]
   
   \[\Rightarrow a^{-1} \in U(R)\]

**Examples**

1. \( U(\mathbb{Z}) = \{ \pm 1 \} \)

2. \( U(\mathbb{Z}_n) = U(n) = \{ a \mid a \text{ mod } n \} \text{ g.c.d. } (a, n) = 1 \)

**Note**

\[a \in \mathbb{Z}_n \implies a^{-1} \in \mathbb{Z}_n\]

\[\iff ax \equiv 1 \pmod{n} \text{ has solution } x\]

\[\iff \text{g.c.d. } (a, n) = 1\]

\[a^x + ny \text{ by Euclid's algorithm}\]
Example 3. \( \mathbb{Z} [x] = \text{ring of polynomials in } 1 \text{ indeterminate with coefficients in } \mathbb{Z} \)

**Elements**
\[
f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0, \quad c_j \in \mathbb{Z}
\]
Define \( \text{degree } f = n \) if \( c_n \neq 0 \)

**Addition**
\[
f(x) = C_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0
g(x) = d_n x^n + d_{n-1} x^{n-1} + \ldots + d_1 x + d_0
\]
\[
(f + g)(x) = (c_n + d_n) x^n + (c_{n-1} + d_{n-1}) x^{n-1} + \ldots + (c_1 + d_1) x + (c_0 + d_0)
\]
\[
(c_j + d_j) \in \mathbb{Z} \text{ if } c_j, d_j \in \mathbb{Z}
\]

**Multiplication is worse**
\[
f(x) \cdot g(x) = (c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0)(d_m x^m + d_{m-1} x^{m-1} + \ldots + d_1 x + d_0)
\]
\[
c_n d_m x^{n+m} + x^{n+m-1} (c_n d_{m-1} + c_{n-1} d_m)
\]
\[
+ \sum_{i+j=k} c_i d_j x^k + \ldots + (c_0 d_0 + c_{n-1} d_1) x + c_0 d_0
\]

These coefficients are in \( \mathbb{Z} \).

Now the other ring properties are not too bad to check. The associative law for multiplication is the worst.

**Extra Credit Exercise**

Complete the proof that \( \mathbb{Z} [x] \) is a commutative ring with unity.
Now what is $U(\mathbb{Z}[x])$?

Suppose $\frac{1}{f(x)} \in \mathbb{Z}[x]$. When is

$$\frac{1}{f(x)} = h(x) \in \mathbb{Z}[x]?$$

Note: usually $\frac{1}{f(x)}$ is an infinite series — not a polynomial. For example:

$$\frac{1}{x-1} = \sum_{n=0}^{\infty} x^n = \text{geometric series}$$

$\notin \mathbb{Z}[x]$.

$$\frac{1}{f(x)} = h(x) \iff 1 = f(x) \cdot h(x)$$

$\Rightarrow \text{degree } (f \cdot h) = 0$

$\Rightarrow \text{degree } f + \text{degree } h = 0$

$\Rightarrow \text{degree } f = \text{degree } h = 0$

So $f$ must be a degree 0 polynomial.

$$f(x) = c_0 \in \mathbb{Z} - \{0\}.$$ And $\frac{1}{f}$ must be in $\mathbb{Z}$.

$$\Rightarrow U(\mathbb{Z}[x]) \equiv U(\mathbb{Z}) = \mathbb{Z}.$$