

Definition 1 — Group of Units.

Let A be a ring. An element $a \in A$ is called a unit if there is an element $b \in A$ such that $a \cdot b = 1$.

We denote the set of all units as following.

$$A^\times := \{ a \in A \mid \exists b \in A : a \cdot b = 1 \} \quad (1)$$

A^\times forms a group.

1. Let $a, b \in A^\times$. Then, there are a' and b' in A^\times such that $a \cdot a' = 1$ and $b \cdot b' = 1$ respectively. We have $a \cdot b \cdot a' \cdot b' = 1$ hence $a \cdot b \in A^\times$. In other words, A^\times is closed under multiplication.
2. Associativity is inherited from the ring A .
3. The identity element is 1. It is included in A^\times as $1 \cdot 1 = 1$. And the identity property $a \cdot 1 = a$ for all $a \in A^\times$ is inherited from A .
4. Let $a \in A^\times$. Then, there is a $b \in A^\times$ such that $a \cdot b = 1$. This b is precisely the inverse element of a .

If A is commutative, then A^\times is commutative.

My guess is that A^\times being a commutative group does not imply that A is commutative.

Also, if A isn't commutative, there probably is a left unit group and a right unit group. Or are they the same?

Examples:

1. $\mathbb{Z}^\times = \{-1, 1\}$
2. For any field \mathbb{K} , it is $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$.
3. Let $A = \text{Mat}_{2 \times 2}(\mathbb{R})$. Then, the group of units A^\times is the set of all invertible matrices also called the general linear group $\text{GL}_2(\mathbb{R})$. This should be true of the general case $A = \text{Mat}_{n \times n}(\mathbb{K})$.
4. Let $\mathbb{Q}[X]$ be a polynomial ring.

Definition 2 — Set of Zero Divisors.

$$\text{ZD}(A) := \{ a \in A \mid \exists b \in A \setminus \{0\} : a \cdot b = 0 \}. \quad (2)$$

Examples:

1. $\text{ZD}(\mathbb{Z}) = \{0\}$.
2. For any field \mathbb{K} , it is $\text{ZD}(\mathbb{K}) = \{0\}$.
- 3.

Proof of above: Let \mathbb{K} be a field and assume there is a nonzero $x \in \mathbb{K}$ such that $x \cdot b = 0$ for a $b \in \mathbb{K}$. The issue here is that \mathbb{K} contains the inverse of b and so we have $x = 0 \cdot b^{-1} = 0$.

Definition 3 — Integral Domain.

A ring A with $\text{ZD}(A) = \{0\}$ is called an integral domain.

Definition 4 — Set of Nilpotent Elements.

$$\text{Nil}(A) := \{ a \in A \mid \exists n \in \mathbb{N} : a^n = 0 \} \quad (3)$$

Definition 5 — Reduced Ring.

A ring A with $\text{Nil}(A) = \{0\}$ is called a reduced ring.

Here some lemmas.

$A \setminus \text{ZD}(A)$ is a semigroup containing A^\times .

Proof:

1. Let $x, y \in A \setminus \text{ZD}(A)$. Then $x \cdot a \neq 0$ and $y \cdot b \neq 0$ for all $a, b \in A$. Assume there exists a $c \in A$ such that $x \cdot y \cdot c = 0$. This implies $x \cdot c = 0$ or $y \cdot c = 0$, but this is impossible. Conclude $x \cdot y \in A \setminus \text{ZD}(A)$.

2. Let $x \in A^\times$. By definition we have for some $a \in A$ that $x \cdot a = 1$. Assume $x \in \text{ZD}(A)$. Then we have $x \cdot b = 0$ for some $b \in A \setminus \{0\}$. With the previous equation we get

$$x \cdot a = 1 \iff x \cdot a \cdot b = 1 \cdot b \quad (4)$$

$$\iff x \cdot b \cdot a = b \quad (5)$$

$$\iff 0 = b \quad (6)$$

But this is a contradiction. Hence $x \notin \text{ZD}(A)$.

3. We have to prove associativity and the identity element, but both are clear.

More lemma: cancelation lemma, clear.

Here is one interesting:

$\text{Nil}(A)$ is an ideal in A .

Proof. Let $x \in \text{Nil}(A)$ and $a \in A$. Then $x \cdot a \in \text{Nil}(A)$ (duh, obviously).

We have to show that $\text{Nil}(A)$ is an additive subgroup of A .

1. Let $x, y \in \text{Nil}(A)$. Then $a^n = 0$ and $b^m = 0$ for some $n \in \mathbb{N}$. With the binominal theorem we get $(a + b)^{n+m} = 0$

I need the latex thingy for quotient ring.

Another lemma. The set $A_{\text{red}} := A/\text{Nil}(A)$ is a reduced ring.

Proof. Assume there is an $\bar{x} \in \text{Nil}(A_{\text{red}})$ but $\bar{x} \neq 0$. So $\bar{x}^n = 0$ for a suitable $n \in \mathbb{N}$. We have $0 = \bar{x}^n = (x + \text{Nil}(A))^n =$

Definition 6 — Sum of Ideals.

Let A be a ring and $\{\mathfrak{a}_i\}_{i \in I}$ be a collection of ideals. We define the smallest ideal in A which contains each \mathfrak{a}_i by $\sum_{i \in I} \mathfrak{a}_i$, i.e.

$$\sum_{i \in I} \mathfrak{a}_i := \left\{ \sum_{i \in I} a_i \mid a_i \in \mathfrak{a}_i \text{ for all } i \in I, \text{ and } a_i = 0 \text{ for almost all } i \right\} \quad (7)$$

This makes sense to me.

Definition 7 — Intersection of Ideals.

We define the largest ideal in A containing each \mathfrak{a}_i by

$$\bigcap_{i \in I} \mathfrak{a}_i \quad (8)$$

Definition 8 — Product of Ideals.

Definition 9 — Radical of Ideals.

The radical of an ideal \mathfrak{a} is given by

$$\sqrt{\mathfrak{a}} := \{ b \in A \mid \exists n \in \mathbb{N} : b^n = a \} \quad (9)$$

Again some lemmas.

$\sqrt{\mathfrak{a}}$ is an ideal.

1. We prove that $\sqrt{\mathfrak{a}}$ is an additive subgroup of A .

- (a) Let $x, y \in \sqrt{\mathfrak{a}}$. Then for some $n, m \in \mathbb{N}$ we have that $x^n = y^m = a$. Consider

$$(x + y)^{n+m} \quad (10)$$

This is a sum and product out of the elements in $\sqrt{\mathfrak{a}}$.

- (b) Associativity and identity is inherited.

- (c) Inverse element is clear.

This is also clear.

Alternate way:

If $\mathfrak{a} = A$, then $\sqrt{\mathfrak{a}} = A$ and this is an ideal. Consider the case $\mathfrak{a} \neq A$. Let $\pi : A \rightarrow A/\mathfrak{a}$ be the natural projection. Since A/\mathfrak{a} is an ideal, we can apply the lemma above and we know that $\text{Nil}(A/\mathfrak{a})$ is an ideal.

The point here is that

$$\pi^{-1}(\text{Nil}(A/\mathfrak{a})) = \sqrt{\mathfrak{a}} \quad (11)$$

The Chinese Remainder theorem

Let A be a ring, $n \geq 2$ and $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals in A .

1. If the \mathfrak{a}_i are pairwise coprime, then $\prod_{i=1}^n \mathfrak{a}_i = \bigcap_{i=1}^n \mathfrak{a}_i$

something

Theorem 1 — Universal Property of the Quotient.

For a ring homomorphism $\varphi : R \rightarrow S$, and an ideal $I \subseteq \ker \varphi$, there exists a unique homomorphism $\bar{\varphi} : R/I \rightarrow S$ such that $\bar{\varphi} \circ \pi = \varphi$, where $\pi : R \rightarrow R/I$ is the canonical projection.

Proof. If there is such a $\bar{\varphi}$, then for all $x \in R$ it must satisfy

$$\varphi(x) = \bar{\varphi}(\pi(x)) = \bar{\varphi}(\bar{x}). \quad (12)$$

We just have to make sure that the above $\bar{\varphi}$ is well defined. Let $x, y \in R$ such that $\bar{x} = \bar{y}$, then by definition of the quotient ring we have that $x - y \in \mathfrak{a} \subseteq \ker \varphi$. So $\varphi(x - y) = 0$ and since φ is a ring homomorphism we have $\varphi(x) = \varphi(y)$. \square

Lemma 1 — Prime Ideals and Integral Domains.

\mathfrak{p} is a prime ideal if and only if R/\mathfrak{p} is an integral domain.

Proof. Apparently this is a tautology? See Bosch 41. \square

Lemma 2 — .

\mathfrak{m} is a maximal ideal if and only if R/\mathfrak{m} is a field.

Lemma 3 — .

All maximal ideals are prime ideals.

Lemma 4 — .

Let R be a ring, \mathfrak{a} an ideal in R . Moreover, define the sets

$$X := \{ \text{Ideals in } R/\mathfrak{a} \} \quad (13)$$

$$Y := \{ \mathfrak{b}/\mathfrak{a} \mid \mathfrak{b} \subset R, \mathfrak{b} \supseteq \mathfrak{a} \} \quad (14)$$

<https://math.stackexchange.com/questions/69578/bijection-between-ideals-of-r-i-and-ideals-containing-i?rq=1>