Notes on Ring Theory

Indrjo Dedej

Last revision: 29th February 2024.

Contents

0   Rings and Ideals

Definition 0.1 (Rings)**.** A *ring* is an abelian group $(R, +)$ endowed with another operation
$$\cdot : R \times R \to R, \ (x, y) \to x \cdot y$$
such that $(R, \cdot)$ is a monoid and the *distributive laws* hold:
$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$$
for every $x, y, z \in R$.

Usually one writes 'ab' instead of '$a \cdot b$'. In order to simplify notations, we assume as convention $\cdot$ has precedence on $+$, in this sense: writing

$$ab + cd$$

we exactly mean

$$(ab) + (cd).$$

As we have settled things, a ring R has two sides, the one of group and the one of monoid, coexisting together as stated by distributive laws. The identity of the 'group part' is generically indicated as 0, while the symbol 1 is reserved for the identity of the 'monoid side'. Notice, however, ring axioms does not ensure $0 \neq 1$, as one may expect.

Lemma 0.2. For R ring, $x0 = 0x = 0$ for every $x \in R$.

Proof.
$$x0 = \underbrace{x(0 + 0) = x0 + x0}_{\text{distributive laws}},$$

so $x0 = 0$, since R with $+$ is a group. $\qquad\square$

If $0 = 1$, then R has a unique element (exercise), that is $0 = 1$; clearly, this is an extreme situation. A ring that is a singleton is said *banal*.

Since $(R, +)$ is a group, we write $-x$ the unique element $a \in R$ that satisfies $x + a = a + x = 0$.

Definition 0.3 (Invertible elements)**.** For R ring and $x \in R$, we say x is *invertible* whenever there exists $y \in R$, called *inverse* of x, such that $xy = yx = 1$.

Provided $x \in R$ has an inverse, it is unique and we indicate it as x^{-1} or $\frac{1}{x}$. For R ring, we consider the set of its invertible elements:

$$R^* := \{x \in R \mid x \text{ is invertible}\}.$$

Proposition 0.4. For R ring, R^* with the operation induced by the monoid part of R is a group.

Proof. Above all, R^* is not empty (at least $1 \in R^*$). Any $b \in R^*$ has the inverse b^{-1}, which itself has b as inverse, thus $b^{-1} \in R^*$. Thus, for every $a, b \in R^*$, the element $b a^{-1}$ is the inverse of ab^{-1}, hence it sis invertible. $\square$

Definition 0.5. A ring R is said *commutative* when $xy = yx$ for every $x, y \in R$.

Definition 0.6 (Fields)**.** A *field* is a non banal and commutative ring whose all non zero elements invertible.

Definition 0.7 (Zero divisors)**.** Let R be a ring. An element $x \in R \smallsetminus \{0\}$ is said *divisor of zero* whenever there exist $y \in R \smallsetminus \{0\}$ such that $xy = yx = 0$.

Proposition 0.8. In a ring, invertible elements are not divisors of zero.

Proof. ... $\square$

Definition 0.9 (Integrity domains)**.** An *integrity domain* is a non banal and commutative ring devoid of divisors of zero.

Lemma 0.10. For R ring and $x \in R \smallsetminus \{0\}$ non divisor of zero. Then

$$\phi_x : R \to R, \ \phi_x(y) := xy$$

is a injective (group) endomorphism on the group side of R.

Proof. ϕ_x is an endomorphism by distributive laws. To prove injectivity, we examine the kernel of ϕ_x:

$$\ker \phi_x = \underbrace{\{y \in R \mid xy = 0\}}_{x \text{ is not a divisor of zero}} = \{0\}. \qquad \square$$

Proposition 0.11. A finite integrity domain is a field.

Proof. Let R be a finite integrity domain: we have to show that every $x \in R \smallsetminus \{0\}$ is invertible. Since x is not a divisor of zero, then consider the injective endomorphism ϕ_x of the previous lemma: since R is finite, ϕ_x must be surjective too. In particular, $\phi_x(y) = xy = 1$ for some $y \in R$. $\square$