

## 2. Constructions and properties related to rings (Chapters 9.4-9.5)

$R = (R, +, \cdot)$  - ring

Definition 2.1 A subset  $S \subseteq R$  is called a subring if  $(S, +|_S, \cdot|_S)$  is a ring.

Remark 2.2. (1)  $R$  and  $\{0\}$  are always subrings of  $R$ .  
(2) A subring of  $R$  may or may not be unital independently of whether  $R$  is or is not unital.

Proposition 2.3. Let  $\emptyset \neq S \subseteq R$ . Then  $S$  is a subring if and only if for all  $x, y \in S$  we have  $x - y \in S$  and  $xy \in S$ .

Proof. ( $\Leftarrow$ ) Follows by definition.

( $\Rightarrow$ ) Since  $x - y \in S \ \forall x, y \in S$ , we have that  $(S, +|_S)$  is an additive subgroup of  $(R, +)$ . Since  $xy \in S$  for all  $x, y \in S$ , we have that  $(S, \cdot|_S)$  is a semigroup. Since distributivity holds in all of  $R$ , it also holds in  $S$  and so  $(S, +|_S, \cdot|_S)$  is a ring.  $\square$

Definition 2.4. The set  $Z(R) = \{r \in R \mid rx = xr \ \forall x \in R\}$  is called the center of the ring  $R$ .

Theorem 2.5.  $Z(R)$  is a subring of  $R$ .

Proof. Clearly  $0 \in Z(R)$  and so  $Z(R) \neq \emptyset$ . We use Proposition 2.3. Let  $r, s \in Z(R)$  so that

$$rx = xr, \quad sx = xs \quad \text{for all } x \in R. \quad (*)$$

Then  $\forall x \in R$  we have

$$(r-s)x = rx - sx \stackrel{(*)}{=} xr - xs = x(r-s)$$

and so  $r-s \in Z(R)$ . Also  $\forall x \in R$  we have

$$(rs)x = r(sx) = r(xs) = (rx)s = (xr)s = x(rs)$$

and so  $rs \in Z(R)$ . It follows by Proposition 2.3 that  $Z(R)$  is a subring of  $R$ .  $\square$

Definition 2.6. Let  $S \subseteq R$ . The smallest subring of  $R$  containing  $S$  is called the subring generated by  $S$ .

Notice that by Proposition 2.3 the intersection of two subrings of  $R$  is again a subring of  $R$ . Hence the subring generated by  $S \subseteq R$  is given by  $\bigcap_{\substack{S \subseteq T \subseteq R \\ T \text{ subring}}} T$ .

Example 2.7 (1) The subring generated by  $S = \emptyset$  is  $\{0\}$ .

(2) The subring generated by  $S = \{a\} \subseteq R$  is  $\{n_1 a + n_2 a^2 + \dots + n_k a^k \mid n_i \in \mathbb{Z}, k > 0\}$  (exercise).

Definition 2.8. The characteristic of  $R$ , denoted  $\text{char}(R)$  is defined to be the minimum positive integer  $n$  such that  $nr = 0 \forall r \in R$ , if such  $n$  exists, and 0 otherwise.

Example 2.9 (1)  $\text{char}(\mathbb{Z}) = 0$ .

(2) Let  $R$  be a unital ring. If  $\text{char}(R) \neq 0$ , then  $\text{char}(R) = \min\{n > 0 \mid n \cdot 1 = 0\}$  (exercise).

(3)  $\text{char}(\mathbb{Z}/(n)) = n$  (exercise).

Theorem 2.10. Assume that  $R$  is a unital integral domain. Then  $\text{char}(R) = 0$  or  $\text{char}(R)$  is prime.

Proof. Assume  $\text{char}(R) = n > 0$ . Then  $n \cdot 1 = 0$ . Let  $d$  be a divisor of  $n$ . Then  $(d \cdot \frac{n}{d}) \cdot 1 = 0 \Rightarrow (d \cdot 1) (\frac{n}{d} \cdot 1) = 0 \Rightarrow d \cdot 1 = 0$  or  $\frac{n}{d} \cdot 1 = 0$ . By minimality of  $n$  we conclude that either  $d = n$  or  $d = 1$  and so  $n$  is prime.  $\square$