

**Definition.** A **ring** is a nonempty set  $R$  together with 2 binary operations (usually denoted by addition and multiplication) such that

1.  $(R, +)$  is an abelian group.
2. Multiplication is associative.
3.  $\forall a, b, c \in R, a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$ .

If, in addition,

4.  $\forall a, b \in R, ab = ba$ ,

then  $R$  is a **commutative ring**. If

5.  $R$  contains a multiplicative identity,  $1$ ,

then  $R$  is a **ring with 1** (or **ring with identity** or **ring with unity**).

**Definition.** A nonzero element  $a$  in a ring  $R$  is a **zero divisor** if there exists a nonzero element  $b \in R$  s.t.  $ab = 0$  or  $ba = 0$ .

**Definition.** An element  $u$  in a ring  $R$  is a **unit** if  $u$  has a multiplicative inverse in  $R$ .

**Definition.** A commutative ring  $R$  with  $1 \neq 0$  and no zero divisors is an **integral domain**.

**Definition.** A ring  $D$  with  $1 \neq 0$  in which every nonzero element is a unit is a **division ring** (or **skew field**).

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

**Definition.** A function  $\phi : R \rightarrow S$  from a ring  $R$  to a ring  $S$  is a **ring homomorphism** if  $\forall a, b \in R$ ,

$$\begin{aligned}\phi(a + b) &= \phi(a) + \phi(b) \text{ and} \\ \phi(ab) &= \phi(a)\phi(b).\end{aligned}$$

**Definition.** The **kernel** of a ring homomorphism  $\phi : R \rightarrow S$  is

$\ker \phi = \{a \in R \mid \phi(a) = 0\}$ .

**Definition.** Let  $R$  be a ring. If there is a positive integer  $n$  s.t.  $\forall a \in R, na = 0$ , then the least such positive integer is the **characteristic** of  $R$ . If no such  $n$  exists, then  $R$  has **characteristic 0**.

**Notation.**  $\text{char}(R) = n$ .

**Definition.** Let  $F \subseteq E$  be fields and  $\alpha \in E$ . The ring homomorphism  $\phi_\alpha : F[x] \rightarrow E$  given by  $p(x) \mapsto p(\alpha)$  is called an **evaluation homomorphism**.

**Division Algorithm.** Let  $F$  be a field and  $f, g \in F[x]$  be nonzero polynomials. Then there exist unique  $q, r \in F[x]$  such that  $f = gq + r$  and  $\deg r < \deg g$ .

**Definition.** Let  $F$  be a field. A nonconstant polynomial  $f(x) \in F[x]$  is **irreducible over  $F$**  (or **irreducible in  $F[x]$** ) if in any factorization  $f = gh$  in  $F[x]$ , either  $g$  or  $h$  is a unit.

**Eisenstein's Criterion for Irreducibility.** Let  $p$  be a prime and  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ . If  $a_n \not\equiv 0 \pmod{p}$ ,  $a_i \equiv 0 \pmod{p}$  for  $i < n$ , and  $a_0 \not\equiv 0 \pmod{p^2}$ , then  $f$  is irreducible over  $\mathbb{Q}$ .

**Definition.** A subring  $N \subseteq R$  of a ring  $R$  is an **ideal** provided for all  $a \in R$ ,  $aN \subseteq N$  and  $Na \subseteq N$ .

**Definition.** Let  $R$  be a ring, let  $X \subseteq R$ , and let  $\{A_i \mid i \in I\}$  be the family of all ideals in  $R$  which contain  $X$ . Then  $\bigcap_{i \in I} A_i$  is the **ideal generated by  $X$** , denoted  $\langle X \rangle$ .

**Definition.** An ideal  $\langle x \rangle$  generated by a single element is called a **principal**

**ideal.**

**Definition.** An ideal  $M \neq R$  in a ring  $R$  is **maximal** if for every ideal  $I$  with  $M \subseteq I \subseteq R$ , either  $I = M$  or  $I = R$ .

**Definition.** Let  $R$  be a commutative ring, and  $P \neq R$  be an ideal.  $P$  is **prime** provided for all  $a, b \in R$ , if  $ab \in P$  then either  $a \in P$  or  $b \in P$ .

**Definition.** The fields  $\mathbb{Z}_p$  and  $\mathbb{Q}$  are called **prime fields**.

**Definition.** Let  $D$  be an integral domain, and  $a, b \in D$ . Then  $a$  **divides**  $b$ , written  $a \mid b$ , if  $\exists c \in D$  such that  $ac = b$ .

**Definition.** Let  $D$  be an integral domain. Two elements  $a, b \in D$  are **associates** in  $D$  if there exists a unit  $u \in D$  such that  $a = bu$ .

**Definition.** Let  $D$  be an integral domain. A nonzero nonunit  $p$  is an **irreducible** of  $D$  if in any factorization  $p = ab$  in  $D$ , either  $a$  or  $b$  is a unit.

**Definition.** Let  $D$  be an integral domain. A nonzero nonunit  $p$  is **prime** if whenever  $p \mid ab$ , either  $p \mid a$  or  $p \mid b$ .

**Definition.** Let  $D$  be an integral domain.  $D$  is a **unique factorization domain** (UFD) if the following two conditions are satisfied:

1. Every nonzero nonunit in  $D$  can be factored into a product of a finite number of irreducibles.
2. If  $p_1 \dots p_r$  and  $q_1 \dots q_s$  are two factorizations of the same element of  $D$  into irreducibles, then  $r = s$  and the  $q_j$  can be renumbered so that the  $p_i$  and  $q_j$  are associates.

**Definition.** Let  $D$  be an integral domain.  $D$  is a **principal ideal domain**

(PID) if every ideal in  $D$  is a principal ideal.

**Definition.** Let  $D$  be a UFD and  $f(x) = a_0 + a_1x + \dots + a_nx^n \in D[x]$ . Then  $f$  is **primitive** if the only common divisors of  $\{a_0, a_1, \dots, a_n\}$  are units of  $D$ .

**Definition.** Let  $D$  be an integral domain. A **Euclidean valuation** on  $D$  is a function  $\nu : D - \{0\} \rightarrow \mathbb{N}$  satisfying the following:

1.  $\forall a, b \in D$  with  $b \neq 0$ ,  $\exists q, r \in D$  such that  $a = bq + r$  with either  $r = 0$  or  $\nu(r) < \nu(b)$ .

2.  $\forall a, b \in D - \{0\}$ ,  $\nu(a) \leq \nu(ab)$ .

**Definition.** Let  $D$  be an integral domain.  $D$  is a **Euclidean domain** if there exists a Euclidean valuation on  $D$ .

**Definition.** Let  $R$  be a commutative ring and  $X \subseteq R$ ,  $X \neq \emptyset$ . An element  $d \in R$  is a **greatest common divisor** (gcd) of  $X$  if

- (i)  $\forall a \in X$ ,  $d \mid a$ , and
- (ii) if  $\forall a \in X$ ,  $c \mid a$ , then  $c \mid d$ .

**Definition.** A **vector space**  $V$  over a field  $F$  consists of an abelian group  $(V, +)$  together with an operation of scalar multiplication  $F \times V \rightarrow V$  such that  $\forall a, b \in F$  and  $\forall \alpha, \beta \in V$ ,

- 1.  $a\alpha \in V$
- 2.  $a(b\alpha) = (ab)\alpha$
- 3.  $(a + b)\alpha = a\alpha + b\alpha$
- 4.  $a(\alpha + \beta) = a\alpha + a\beta$
- 5.  $1\alpha = \alpha$

**Definition.** Let  $V$  be a vector space over a field  $F$ , and let  $X \subseteq V$ . The **span** of  $X$  consists of all (finite) **linear combinations**  $a_1x_1 + a_2x_2 + \dots + a_nx_n$ , where  $x_i \in X$  and  $a_i \in F$ .

**Definition.** Let  $V$  be a vector space over a field  $F$ , and let  $X \subseteq V$ .  $X$  is a **linearly independent** set if for all distinct  $x_1, x_2, \dots, x_n \in X$  and all  $a_i \in F$ ,  
 $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0 \Rightarrow \forall i, a_i = 0$ .

**Definition.** Let  $V$  be a vector space over a field  $F$ , and let  $X \subseteq V$ .  $X$  is a **basis** for  $V$  over  $F$  if  $X$  is a linearly independent spanning set for  $V$ .

**Definition.** Let  $V$  be a vector space over a field  $F$ , and assume  $V$  has a finite basis over  $F$ . Then the **dimension** of  $V$  over  $F$  is the number of elements in this basis. (Note: The number of elements in *any* basis of  $V$  over  $F$  is the same.)

**Definition.** A field  $E$  is an **extension field** of a field  $F$  if  $F$  is a subfield of  $E$ .

**Definition.** Let  $F \leq E$  be fields. An element  $\alpha \in E$  is **algebraic over  $F$**  if there exists a nonzero  $f(x) \in F[x]$  such that  $f(\alpha) = 0$ . If no such  $f(x)$  exists, then  $\alpha$  is **transcendental over  $F$** .

**Definition.** A **monic** polynomial is a polynomial whose leading coefficient is 1.

**Definition.** Let  $F \leq E$  be fields and  $\alpha \in E$  be algebraic over  $F$ . Then  $\text{irr}(\alpha, F)$  is the unique monic polynomial in  $F[x]$  having  $\alpha$  as a zero. The degree of  $\text{irr}(\alpha, F)$  is  $\deg(\alpha, F)$ .

**Definition.** Let  $F \leq E$  be fields.  $E$  is a **simple extension** of  $F$  if  $\exists \alpha \in E$  such that  $E = F(\alpha)$ .

**Definition.** Let  $F \leq E$  be fields.  $E$  is an **algebraic extension** of  $F$  if every element of  $E$  is algebraic over  $F$ .

**Definition.** Let  $F \leq E$  be fields. Then  $\overline{F}_E = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$  is the **algebraic closure of  $F$  in  $E$** .

**Definition.** A field  $F$  is **algebraically closed** if every nonconstant polynomial in  $F[x]$  has a zero in  $F$ .

**Definition.** An element  $\alpha$  of a field  $F$  is an  **$n$ th root of unity** if  $\alpha^n = 1$ . It is a **primitive  $n$ th root of unity** if  $\alpha^n = 1$  and  $\alpha^m \neq 1$  for  $0 < m < n$ .

**Definition.** An **isometry** of  $\mathbb{R}^2$  is a bijection  $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  such that  $\forall P, Q \in \mathbb{R}^2, d(\phi(P), \phi(Q)) = d(P, Q)$ .

**Definition.** Let  $\mathcal{J}$  be the group of isometries of  $\mathbb{R}^2$  and  $A \subseteq \mathbb{R}^2$ . Define  $\mathcal{J}_A = \{\phi \in \mathcal{J} \mid \phi(A) = A\}$ .

**Remark.**  $\mathcal{J}$  consists of translations, rotations, reflections, and glide reflections.

**Definition.** A **discrete frieze** is a pattern of the form  $\mathbb{Z} \times B \subseteq \mathbb{R}^2$ , where  $B$  is a bounded set of diameter less than 1.

**Definition.** If  $A$  is a discrete frieze, then  $\mathcal{J}_A$  is a **discrete frieze group**.

**Definition.** If  $F \leq E$  are fields, then  $\text{Aut}_F E = \{\sigma \in \text{Aut} E \mid \sigma|_F = \mathbb{1}_F\}$ .

**Notation.**  $G(E/F) = \text{Aut}_F E$ .

**Definition.** Let  $E$  be an extension field of a field  $F$ , and let  $\alpha, \beta \in E$ .  $\alpha$  and  $\beta$  are **conjugate over  $F$**  if  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$ .

**Definition.** Let  $E$  be an extension field of a field  $F$ , and let  $\alpha$  and  $\beta$  be

conjugate over  $F$ , with  $\deg(\alpha, F) = n$ . The isomorphism  $\psi_{\alpha, \beta} : F(\alpha) \rightarrow F(\beta)$  given by  $(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}) \mapsto c_0 + c_1\beta + \dots + c_{n-1}\beta^{n-1}$  is called a **conjugation isomorphism**.

**Definition.** Let  $A \subseteq X$  and  $f : A \rightarrow Y$  be a map in any category. Then a map  $g : X \rightarrow Y$  **extends**  $f$  (or is an **extension** of  $f$ ) if  $g|_A = f$ .

**Definition.** Let  $E$  be a finite extension of the field  $F$ . Then the number of extensions of any isomorphism  $\sigma : F \rightarrow F'$  to  $E$  is the **index of  $E$  over  $F$** ,  $\{E : F\}$ .

**Definition.** Let  $F \leq K$  be fields and  $H \leq \text{Aut}_F K$ . Then  $\gamma(H) = \{a \in K \mid \forall \sigma \in H, \sigma(a) = a\}$  is the **fixed field of  $H$  in  $K$** .

**Note.** If  $F \leq E \leq K$  are fields, then  $\lambda(E) = \{\sigma \in \text{Aut}_F K \mid \forall a \in E, \sigma(a) = a\}$  is a subgroup of  $\text{Aut}_F K$ . Note that  $\lambda(E) = \text{Aut}_E K$ .