- K <u>corps commutatif</u> ie anneau commutatif unitaire $(K,+,\bullet)$

  • <u>anneau commutatif unitaire</u> si Def 2.65

  (a) $(K,+)$ est un groupe Abelien (ie groupe commutatif)

  (b) la multiplication est associative et commutative

  • $\forall (x,y,z)\in K^3 \quad (x\bullet y)\bullet z = x\bullet(y\bullet z)$

  • $\forall (x,y)\in K^3 \quad x\bullet y = y\bullet x$

  (c) la multiplication est distributive sur l'addition

  $\forall (x,y,z)\in K^3 \quad x\bullet(y+z) = (x\bullet y)+(x\bullet z)$

  (d) la multiplication admet un élément neutre $1\in K$

  $\forall x\in K \quad 1\bullet x = x\bullet 1 = x$

  • $(K,\square,\blacktriangle)$ est un <u>groupe commutatif</u> ou <u>groupe Abélien</u> (K un ensemble et $\square: K\times K\to K$ operation binaire)
  Def 2.43

  * $(K,\square)$ est un groupe si

  (a) associatif : $\forall (x,y,z)\in K \quad (x\square y)\square z = x\square(y\square z)$

  (b) admet un élément neutre : $\exists e\in K,\ \forall x\in K,\ e\square x = x\square e = x$

  (c) inverse : $\forall x\in K \quad \exists y\in K \quad x\square y = e = y\square x$

  * $(K,\square)$ est un groupe commutatif si (

  (a) $(K,\square)$ est un groupe

  (b) commutatif : $\forall (x,y)\in K^2,\ x\square y = y\square x$

- S est un <u>sous-corps</u> de $(K,+,\bullet)$ corps commutatif d'unité $1\in K$ si
  Def 3.2

  (a) $\forall (x,y)\in S \quad x+y\in S$ et $x\bullet y\in S$

  (b) Si $a\in S$ alors $-a\in S$

  (c) si $a\in S^*$ alors $a^{-1}\in S$ (ie a^{-1} est l'unique élément de S tq $a\bullet a^{-1}=1$)
  Def 2.68

  (d) $1\in S$

- $(K,+,\bullet)$ anneau commutatif unitaire $a\in K$

  • élément neutre pour + noté 0 : $0+a = a+0 = a$

  • élément neutre pour • : 1 $\quad 1\bullet a = a\bullet 1 = a$

  • inverse pour l'addition est unique noté $-a$: $a+(-a) = 0 = (-a)+a$
  • inverse pour la multiplication est unique noté a^{-1} : $a\bullet(a^{-1}) = 1$

Soient K et L deux corps commutatifs.

On dit que $f : K \to L$ est un homomorphisme de corps si

(a) $\forall (a,b) \in K^2$, $f(a+b) = f(a) + f(b)$ (compatibilité addition)

(b) $\forall (a,b) \in K^2$, $f(ab) = f(a) \cdot f(b)$ (compatibilité multiplication)

(c) $f(1_K) = 1_L$ $1_K \in K$ et $1_L \in L$ unités.

On dit que $f : K \to L$ est un isomorphisme de corps si

$\exists g : L \to K$ un homomorphisme de corps tq $g \circ f = id_K$ et $f \circ g = id_L$

Lorsque $K = L$, un isomorphisme de corps $K \to K$ est appelé un automorphisme du corps K