Corpuri

Def. Un inel unitar K cu $1 \neq 0$ s.n. __corp__ dc. orice elem. $\neq 0$ este inversabil.
Dc. înmulțirea este comutativă, at. corpul s.n. __corp comutativ__.

Ex. 1) $\mathbb{Q}, \mathbb{R}$ corpuri comutative

2) $\mathbb{Z}_n$ corp $\Longleftrightarrow$ n nr. prim

3) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ corp comut.

4) Orice inel unitar integru și finit este corp.

Prop. R inel unitar, $1 \neq 0$.
R este corp $\Longleftrightarrow$ $\{0\}$ și R sunt singurele ideale stângi ale lui R.

Def. K corp, $K' \subset K$, $K' \neq \emptyset$. K' s.n. __subcorp__ dc. $(K', +, \cdot)$ este corp. În acest caz se mai spune că K este o __extindere__ a lui K'.

Prop. K corp, $K' \subset K$, $K' \neq \emptyset$. At. K' este subcorp al lui K dc. și numai dc.

1) $(\forall)\, x, y \in K' \Rightarrow x - y \in K'$;

2) $(\forall)\, x, y \in K'$, $x \neq 0 \Rightarrow x^{-1}y \in K'$.

Ex. 1) $\mathbb{Q} \subset \mathbb{R}$ subcorp. (__$K \subset K$ subcorp__)

2) $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ subcorp.

3) $\mathbb{Z}_p$ și $\mathbb{Q}$ nu au subcorpuri proprii.

Def. K, K' corpuri, $f : K \to K'$ funcție.
f s.n. __morfism de corpuri__ dc.

$$f(x+y) = f(x) + f(y)$$
$$f(xy) = f(x) f(y) \quad (\forall)\, x, y \in K$$
$$f(1) = 1'$$

Obs. 1) f este morfism de corpuri dc. este morfism unitar de inele.
2) $f(x^{-1}) = (f(x))^{-1}$, $(\forall)\, x \in K^*$.

Prop. Orice morf. de corpuri este injectiv.

Lemă K corp, $K'_\alpha \subset K$, $\alpha \in A$ subcorpuri

$$\Rightarrow \bigcap_{\alpha \in A} K'_\alpha \subset K \text{ subcorp.}$$

Obs. Dc. considerăm intersecția tuturor subcorpurilor unui corp obț. un corp care nu are subcorpuri proprii.

Def. Un corp care nu are subcorpuri proprii s.n. corp prim.

Obs. 1) Orice corp conține ca subcorp un corp prim.
2) $\mathbb{Z}_p$, $\mathbb{Q}$ corpuri prime.

Prop. Orice corp prim este izomorf cu $\mathbb{Q}$ sau cu un $\mathbb{Z}_p$, p prim.

Dem. K corp prim, $\varphi : \mathbb{Z} \to K$, $\varphi(n) = n \cdot 1_K$.
φ morf. de inele
$\ker\varphi = (0) \Rightarrow \varphi$ inj. $\Rightarrow \mathbb{Z} \simeq \varphi(\mathbb{Z}) \subset K \Rightarrow K \simeq \mathbb{Q}$.
$\ker\varphi = p\mathbb{Z} \Rightarrow \mathbb{Z}/p\mathbb{Z} \simeq \operatorname{Im}\varphi \subset K \Rightarrow \mathbb{Z}/p\mathbb{Z}$ integru
$\Rightarrow \mathbb{Z}/p\mathbb{Z}$ corp $\Rightarrow K \simeq \mathbb{Z}/p\mathbb{Z}$. //

Def. Fie K un corp. Dc. K conține un subcorp prim izomorf cu $\mathbb{Q}$, at. spunem că K are caracteristica zero și scriem $\boxed{\operatorname{char} K = 0.}$

Dc. K conține un subcorp prim izomorf cu un $\mathbb{Z}_p$, at. spunem că K are caracteristica p și scriem $\boxed{\operatorname{char} K = p.}$

Obs. 1) $\operatorname{char} K = \operatorname{ord}(1_K)$ în grupul $(K,+)$.

2) Dc. $K \subset L$ ext. de corpuri, at. $\operatorname{char} K = \operatorname{char} L$.

Exemple 1) $\operatorname{char} \mathbb{Q} = 0$, $\operatorname{char} \mathbb{Z}_p = p$

2) Din Obs. 2) rezultă $\operatorname{char} \mathbb{R} = 0$, $\operatorname{char} \mathbb{Q}(\sqrt{2}) = 0$.

Vom construi acum trei exemple importante de corpuri.

① Corpul nr. complexe

Fie $\mathbb{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$.

$\mathbb{C}$ este corp comutativ în raport cu adunarea și înmulțirea matricelor.

Avem un morf. de corpuri

$$f : \mathbb{R} \longrightarrow \mathbb{C},$$

$f(a) = aI_2$. Astfel putem identifica pe $\mathbb{R}$ cu un subcorp al lui $\mathbb{C}$.

Fie $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. At. $i^2 = -1$ iar

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a\cancel{I_2} + bi.$$

Deci $\mathbb{C}=\{a+bi \mid a,b\in\mathbb{R}\}$ cu adunarea și înmulțirea date astfel:

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$
$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

(II) Corpul cuaternionilor

Fie $\mathbb{H}=\left\{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a}\end{pmatrix} \mid a,b\in\mathbb{C}\right\}$.

$\mathbb{H}$ este corp necomutativ în raport cu adunarea și înmulțirea matricelor. Elementele lui $\mathbb{H}$ s.n. cuaternioni.

Avem un morfism de corpuri

$$f:\mathbb{C}\to\mathbb{H},$$

$f(a)=\begin{pmatrix} a & 0 \\ 0 & \bar{a}\end{pmatrix}$ care ne permite să identificăm pe $\mathbb{C}$ cu un subcorp al lui $\mathbb{H}$. Astfel orice nr. real a se identifică cu $\begin{pmatrix} a & 0 \\ 0 & a\end{pmatrix}$ iar i se identifică cu $\begin{pmatrix} i & 0 \\ 0 & -i\end{pmatrix}$.

Considerăm cuaternionii $j=\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}$ și $k=\begin{pmatrix} 0 & i \\ i & 0\end{pmatrix}$. Dc. $a=x+iy$, $b=z+it$, cu $x,y,z,t\in\mathbb{R}$, at.

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a}\end{pmatrix}=x+iy+jz+kt.$$

Deci $\mathbb{H}=\{x+iy+jz+kt \mid x,y,z,t\in\mathbb{R}\}$ și avem relațiile:

$$\begin{cases} ij=k, & ji=-k \\ jk=i, & kj=-i \\ ki=j, & ik=-j \\ i^2=j^2=k^2=-1. \end{cases}$$

Obs. Cuaternionii $\{\pm 1, \pm i, \pm j, \pm k\}$ formează grup necomutativ în raport cu înmulțirea numit grupul cuaternionilor.

III Corpul de fracții al unui domeniu de integritate

Este evident că orice corp comutativ este un domeniu de integritate, dar nu și invers.
Fie R domeniu. Îi vom asocia lui R un corp comutativ care îl conține pe R ca subinel și-l vom numi corpul de fracții al lui R.

Să considerăm produsul cartezian

$$R \times R^* = \{(a, b) \mid a \in R, b \in R, b \neq 0\}.$$

Pe ac. mulțime def. o relație binară astfel: $(a, b) \sim (c, d) \iff ad = bc$.
"$\sim$" este o relație de echivalență.
Fie $K = R \times R^* / \sim$. Clasa de echivalență a unei perechi (a, b) se va nota $\frac{a}{b}$ și se va numi fracție.
Definim pe K două operații algebrice

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Acestea sunt bine definite și $(K,+,\cdot)$ este un corp comutativ.

Def K s.n. corpul de fracții al lui R și se not. $Q(R)$.

Avem un morfism injectiv de inele

$$f : R \to K$$

$f(a) = \frac{a}{1}$.

Exemple $Q(\mathbb{Z}) = \mathbb{Q}$, $Q(\mathbb{Z}[i]) = \mathbb{Q}[i]$, $Q(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}]$.

$(\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$, $\mathbb{Q}[i] = \{a+bi \mid a,b \in \mathbb{Q}\})$

$(\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$, $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\})$