Teoria corpurilor

Plan : definitie grupuri(+ordin, grup finit, subgrup, subgrup generat de x \in G, grup cyclic), inele(Definitie, domeniu de integritate, idealuri, ), corpuri spatii vectoriale,

\chapter{Structuri Algebrice de baza}

\section{Grupuri}

\label{sec:sec01}

\begin{dfn}

Un grup reprezinta o multime $S$ impreuna cu o operatie de compozitie $\cdot$ astfel incat sunt respectate urmatoarele reguli:

\\ - legea $\cdot$ e asociativa $\rightarrow$ $\forall x, y, z\in S: (x\cdot y)\cdot z = x\cdot (y \cdot z)$

\\ - existanta unui element neutru, unic $\rightarrow$ $\exists e\in S: x \cdot e = x, \forall x\in S$

\\ - $\forall x\in S, \exists y\in S$, numit invers al elementului $x$, astfel incat $x\cdot y = y\cdot x = e$

\end{dfn}

\begin{dfn}

Se numeste grup abelian, acel grup in care legea de compozitie $\cdot$ este de asemenea comutativa, adica pentru orice doua elemente

$x, y \in S$ avem $x \cdot y = y \cdot x$

\end{dfn}

\begin{dfn}

Fie $G$ un grup si H o submultime a lui $G$. $H$ este un subgrup a lui $G$ daca sunt indeplinite conditiile:

\\ -inchidere la operatia de compozitie $\rightarrow$ $\forall x, y \in H, x \cdot y \in H$

\\ - daca $x \in H \Rightarrow x^{-1} \in H$

\end{dfn}

\begin{dfn}

Se numeste ordin al grupului $G$, cardinalul multimii G, notat $|G|$. Pentru un element $g \in G$, se numeste ordin al lui $g$, cel mai

mic intreg $n$ astfel incat $g^n = e$, unde $e$ este element netru al lui $G$. Altfel spunem ca ordinul lui $g$ este infinit.

\end{dfn}

\begin{dfn}

Fie $G$ un grup si $g \in G$. Se numeste subgrup generat de $g$ multimea $\set{g^n\mid n\in \mathbb{Z}}$ si se noteaza $\langle g \rangle$. Daca $G = \langle g \rangle$ atunci $G$ se numeste grup ciclic iar $g$ generator pentru $G$.

\end{dfn}

%=======

\section{Inele}

\label{sec:sec02}

\begin{dfn}

Un inel reprezinta un triplet $(R, +, \cdot)$, unde $R$ este o multime iar $+, \cdot$ reprezinta 2 legi de compozitie. Urmatoarele proprietati trebuiesc simultan indeplinite:

\\ - $(R, +)$ reprezinta un grup abelian

\\ - $x \cdot y = y \cdot x, \forall x,y\in R$ si de asemenea exista element neutru la inmultire, diferit de elementul neutru la adunare

\\ - legea $\cdot$ este distributiva fata de $+$, adica $\forall x,y,z\in R, x\cdot (y + z) = x\cdot y + x\cdot z \land (y + z)\cdot x = y\cdot x + z\cdot x$

\end{dfn}

\begin{dfn}

Fie $R$ un inel. $I$ Se numeste ideal a lui $R$ daca $I\subset R, I \neq \emptyset$ si respecta:

\\ - $I$ este un subgrup pentru $(R, +)$

\\ - $\forall x\in R, \forall y\in I \Rightarrow x\cdot y, y\cdot x \in I$

\end{dfn}

\begin{obs}

Fie $\Psi$ un homomorfism de la $\mathbb{Z}$ la un inel $R$ definit astfel:

\\ $\Psi (n) = \begin{cases}

1+...+1 & $de n ori daca $n\geq 0 \\

-(1+...+1) & $de -n ori altfel $

\end{cases}$

\end{obs}

Kernelul lui $\Psi$ este un ideal a lui $\mathbb{Z}$ si daca toti multipli de 1 sunt diferiti atunci $ker\Psi = {0}$. Altfel, daca $R$ este finit de exemplu, cativa multiplii vor fi $0$. Altfel spus, kernelul lui $\Psi$ este generat de un numar natural $m$

\begin{dfn}

Fie $R$ un inel si $\Psi$ definit ca mai sus. Kernelul lui $\Psi$ are forma $m\mathbb{Z}, m\in\mathbb{N}$. $m$ poarta denumirea de caracterisica a inelului $R$ si se noteaza $char(R)$

\end{dfn}

\begin{dfn}

Fie $R$ un inel. Un element $x\in R$ este inversabil daca $\exists! y\in R, x\cdot y = y\cdot x = e$. $y$ se numeste unitate. Multimea tuturor unitatilor se noteaza cu $R^{\*}$

\end{dfn}

\begin{dfn}

Fie $n\geq 1$. Notam cu $\phi (n) = |(\mathbb{Z}/n\mathbb{Z})^{\*}|$. Functia $\phi$ se numeste functia lui Euler. Deoarece elementele inversabile din $\mathbb{Z}/n\mathbb{Z}$ ... $\phi (n) = |\set{x\mid 1\leq x\leq n, gcd(x, n)=1}|$

\end{dfn}

\begin{teo}

Fie $n, x$ doua numere intregi astfel incat $gcd(n,x)=1$. Atunci este adevarata relatia:

$x^{\phi(n)}\equiv 1 (mod n)$

\end{teo}

\section{Corpuri}

\label{sec:sec03}

\begin{dfn}

\end{dfn}

\begin{ex}

\end{ex}