Množica $G$ skupaj z binarno operacijo $(x, y) \mapsto xy$ je grupa, če velja (za vse $x, y, z \in G$): 1)$(xy)z = x(yz)$; 2) obstaja enota/element $1 \in G$, da je $1x = x1 = x$; 3) obstaja inverz $x^{-1} \in G$, da je $xx^{-1} = x^{-1}x = 1$. Če velja še $xy = yx$ je to Abelova grupa.

**Primeri grup**

Grupa, ki ima red 1, je trivialna grupa. Bijektivni preslikavi iz množice $X$ v množico $X$ pravimo permutacija množice $X$. Simetrična grupa $Sim(X)$ je grupa permutacij množice $X$. Splošna linearna grupa $GL_n(F) = \{A \in M_n(F) \mid detA \neq 0\}$ je grupa vseh obrnljivih matrik. Diedrska grupa $D_{2n}$ reda $2n$ je grupa simetrij previlnega $n$-kotnika. Velja: $zr = r^{-1}z = r^{n-1}z$ in $zr^k = r^{-k}z$. Množica $G_1 \times \cdots \times G_s$ z vpeljano operacijo ('množenje po komponentah') je direktni produkt grup.

Za neprazno podmnožico $H$ grupe $G$ veljajo ekvivalence: 1) $H$ je podgrupa $G$; 2) za vse $x, y \in H$ je $xy^{-1} \in H$; 3) $H$ je zaprta za množenje in za vsak $x \in H$ je $x^{-1} \in H$. Neprazna končna podmnožica $H$ grupe $G$ je podgrupa natanko tedaj, ko je zaprta za množenje. Podmnožica $H$ grupe $\mathbb{Z}$ je podgrupa za seštevanje natanko tedaj, ko je $H = n\mathbb{Z}$ za nek $n \in \mathbb{N} \cup \{0\}$. Produkt podgrup $H$ in $K$ grupe $G$ je $HK = \{hk \mid h \in H, k \in K\}$. Če je $HK = KH$ je $HK \leq G$. Posebna linearna grupa: $SL_n(F) = \{A \in M_n(F) \mid detA = 1\}$. Ortogonalna grupa: $O_n = \{A \in M_n(\mathbb{R}) \mid AA^t = I\}$. Unitarna grupa: $U_n = \{A \in M_n(\mathbb{C}) \mid AA^* = I\}$. Center grupe $G$ je množica $Z(G) = \{c \in G \mid cx = xc \ za \ \forall x \in G\}$.

Naj bo $H$ podgrupa grupe $G$ in $a \in G$. Množica $aH = \{ah \mid h \in H\}$ je odsek grupe $G$ po podgrupi $H$. Za $a, b \in G$ velja: $aH = bH \Leftrightarrow a^{-1}b \in H$. Za $a, b \in G$ velja: odseka $aH$ in $bH$ sta bodisi enaka bodisi disjunktna. Moči množice vseh odsekov $\{aH \mid a \in G\}$ grupe $G$ po podgrupi $H$ pravimo indeks podgrupe $H$, oznaka $[G : H]$. (Lagrangeov izrek) Za podgrupo $H$ grupe $G$ je $|G| = [G : H] \cdot |H|$. Red vsake podgrupe končne grupe deli red grupe.

**Grupe ostankov in ciklične grupe**

Množica $\mathbb{Z}_n$ s seštevanjem $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$ je Abelova grupa. Podgrupo $\langle a \rangle$ imenujem ciklična grupa, generirana z elementom $a$. Če je $\langle a \rangle = G$ za kak $a \in G$, je $G$ ciklična grupa, $a$ je generator grupe $G$. $a \in G$. Če za $n \in \mathbb{N}$ velja $a^n = 1$, potem rečemo, da ima $a$ končen red, najmanjšemu takemu številu $n$ pa red elementa $a$. Če ima element $a$ grupe $G$ končen red $n$, potem ima ciklična grupa $\langle a \rangle$ red $n$. Končna grupa reda $n$ je ciklična natanko tedaj, ko vsebuje element reda $n$. Red vsakega elementa končne grupe deli red grupe. Če je $G$ končna grupa, je $a^{|G|} = 1$ za vsak $a \in G$. Vsaka grupa $G$ s praštevilskim redom je ciklična; za vsak od 1 različen element $a \in G$ je $\langle a \rangle = G$. Vsaka ciklična grupa je Abelova.

Najmanjšo podgrupo $G$, ki vsebuje podmnožico $X$, označimo z $\langle X \rangle$, in ji pravimo podgrupa, generirana z množico $X$. Če je $\langle X \rangle = G$, rečemo da je grupa $G$ generirana z množico $X$. Elementom $X$ pravimo generatorji grupe $G$, množici $X$ pa grupa generatorjev $G$.

**Definicija kolobarja, obsega in polja**

Množica $K$ skupaj z binarnima operacijama seštevanja $(x, y) \to x + y$ in množenja $(x, y) \to xy$ je kolobar, če velja: $K$ je Abelova grupa za seštevanje; $K$ je monoid za množenje; veljavnost distributivnostnih zakonov: $(x + y)z = xz + yz$ in $z(x + y) = zc + zy$. V poljubnem kolobarju za vse $x, y, z \in K$ velja: 1) $0x = x0 = 0$; 2) $(-x)y = x(-y) = -(xy)$; 3) $(x - y)z = xz - yz$, $z(x - y) = zx - zy$; 4) $(-x)(-y) = xy$; 5) $(-1)x = x(-1) = -x$. Neničeln kolobar je obseg, če je vsak njegov neničeln element obrnljiv. Komutativen obseg imenujemo polje. Element $x$ kolobarja $K$ je delitelj niča, če $x \neq 0$ in če obstaja tak $y \neq 0$ iz $K$, da je $xy = 0$ ali $yx = 0$. Element kolobarja, ki je enak svojemu kvadratu je idempotent. Če je $e$ idempotent ($e^2 = e$), potem je tudi $1 - e$ idempotent. Element $a$ je nilpotenten element oz. nilpotent, če je $a^n = 0$ za nek $n \in \mathbb{N}$. Komutativen kolobar brez deliteljev niča je cel kolobar. Obrnljiv element kolobarja ni delitelj niča. Obsegi so brez deliteljev niča. V kolobarju brez deliteljev niča velja pravilo krajšanja.

**Definicija algebre**

Naj bo $F$ polje. Množica $V$ skupaj z (notranjo) binarno operacijo seštevanja $(u, v) \to u + v$ in zunanjo binarno operacijo iz $F \times V$ v $V$, imenovano množenje s skalarji in označeno $(\lambda, v) \to \lambda v$, je vektorski prostor nad $F$, če velja (za $\forall \lambda, \mu \in F$ in $\forall u, v \in V$): 1) $V$ je Abelova grupa za seštevanje; 2) $\lambda(u + v) = \lambda u + \lambda v$; 3) $(\lambda + \mu)v = \lambda v + \mu v$; 4) $\lambda(\mu v) = (\lambda\mu)v$ in 5) $1v = v$. V vsakem vektorskem prostoru $V$ nad $F$ velja (za vsak $\lambda \in F$ in $v \in V$): 1) $\lambda 0 = 0$; 2) $0v = 0$; 3) $\lambda v = 0 \ \Rightarrow \lambda = 0 \vee v = 0$ in 4) $(-\lambda)v = -(\lambda v) = \lambda(-v)$. Množica $A$ skupaj z binarnima operacijama seštevanja in množenja ter zunanjo operacijo množenja s skalarji se imenuje algebra nad $F$, če velja: 1) $A$ je za seštevanje in množenje s skalarji vektorski prostor nad $F$; 2) $A$ je kolobar za seštevanje in množenje in 3) za vse $\lambda \in F$ in $x, y \in A$ je $\lambda(xy) = (\lambda x)y = x(\lambda y)$. Če je element algebre $a$ obrnljiv, potem ni delitelj niča. Kvaternioni: $\mathbb{H} = \{\lambda_0 1 + \lambda_1 i + \lambda_2 j + \lambda_3 k | \lambda_i \in \mathbb{R}\}$ (4-razsežna algebra, obseg, ni polje /ni komutativno/). Kvaternionska grupa: $Q = \{\pm 1, \pm i, \pm j, \pm k\}$

**Podkolobarji, podalgebre in podpolja**

Podmnožica $L$ kolobarja $K$ je podkolobar kolobarja $K$, če vsebuje enoto 1 kolobarja $K$ in je za isti operaciji tudi sama kolobar. Podobno podalgebre, podprostori, podpolja. Polje $E$ je razširitev polja $F$, če je $F$ podpolje $E$. Podmnožica $L$ kolobarja $K$ je podkolobar natanko tedaj, ko velja: 1) $1 \in L$; 2) $L$ je podgrupa za seštevanje; 3) $L$ je zaprta za množenje. Podmnožica $B$ algebre $A$ je podalgebra natanko tedaj, ko velja: 1) $1 \in B$, 2) $B$ zaprta za seštevanje; 3) $B$ zaprta za množenje; 4) za vsak skalar $\lambda$ in $x \in B$ je $\lambda x \in B$. Podmnožica $F$ polja $E$ je podpolje natanko tedaj, ko velja: 1) $1 \in F$, 2) $F$ je podgrupa za seštevanje; 3) $F$ je zaprta za množenje; 4) za vsak $x \neq 0$ iz $F$ tudi $x^{-1} \in F$. Center kolobarja: $Z(K) = \{c \in K \mid xc = cx \ za \ vsak \ x \in K\}$.

**Kolobarji ostankov in karakteristika kolobarja**

Naj bo $K$ kolobar. Ko obstajajo taka naravna števila $n$, da je $n \cdot 1 = 0$, potem najmanjšemu izmed njih pravimo karakteristika kolobarja $K$. V tem primeru ima $K$ končno karakteristiko. Če takih števil ni, rečemo, da ima $K$ karakteristiko 0. Za kolobar $K$ s karakteristiko $n > 0$ velja: 1) $nx = 0$ za vse $x \in K$; 2) za vsak $m \in \mathbb{Z}$ je $m \cdot 1 = 0$ natanko tedaj, ko $n \mid m$; 3) če $K$ nima deliteljev niča in $K \neq \{0\}$ je $n$ praštevilo. Če v aditivno grupo $\mathbb{Z}_n$ vpeljemo množenje s predpisom $(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = ab + n\mathbb{Z}$, postane $\mathbb{Z}_n$ komutativen kolobar. Končen cel kolobar je polje. Naravno število $p$ je praštevilo natanko tedaj, ko je kolobar $\mathbb{Z}_p$ polje. (Wedderburnov izrek) Vsi končni obsegi so komutativni. (Fermatov mali izrek) Za vsako praštevilo $p$ in vsako naravno število $a$ je $a^p \equiv a \mod p$. (Eulerjev izrek) $k, n \in \mathbb{N}$: $\phi(n) = k$, kjer je $k < n; GCD(n, k) = 1$, tu $k$ predstavlja število vseh tujih števil $n$ manjših od $n$. (Za elemente grupe obrnljivih elementov velja: $red(a) \mid \phi(n)$ in $a^{\phi(n)} = 1 \mod n$)

**Generatorji kolobarjev, algeber in polj**

Naj bo $K$ kolobar in $X$ njegova podmnožica. Podkolobar, generiran z $X$ je najmanjši kolobar, ki vsebuje $X$. Enak je preseku vseh podkolobarjev, ki vsebujejo $X$. Če $X$ sestoji iz elementov $x_i$, rečemo da je $\overline{X}$ podkolobar, generiran z elementi $x_i$. Kadar je $\overline{X} = K$, rečemo, da je $K$ generiran z množico $X$ oziroma, da so elementi $X$ njegovi generatorji. Kolobar je končno generiran, če je generiran s končno množico. Podkolobar, generiran z $X$ je množica vseh elementov oblike $k_1x_{11}\cdots x_{1m_1}+k_2x_{21}\cdots x_{2m_2}+\cdots+k_nx_{n1}\cdots x_{nm_n}$, kjer $x_{ij}\in X\cup\{1\}$ in $k_i\in\mathbb{Z}$. Podalgebra, generirana z $X$ je množica vseh elementov oblike $\lambda_1x_{11}\cdots x_{1m_1}+\lambda_2x_{21}\cdots x_{2m_2}+\cdots+\lambda_nx_{n1}\cdots x_{nm_n}$, kjer $x_{ij}\in X\cup\{1\}$ in $\lambda_i\in F$. Podpolje, generirano z $X$ je množica vseh elementov oblike $uv^{-1}$, kjer je $u,v\in\overline{X}$ in $v\neq 0$.

**Pojem homomorfizma**

(D) Preslikava $\phi: A\to A'$ je homomorfizem grup, če sta $A$ in $A'$ grupi in za vse $x,y\in A$ velja $\phi(xy)=\phi(x)\phi(y)$. (D) Preslikava $\phi: A\to A'$ je homomorfizem algeber, če sta $A$ in $A'$ algebri nad istim poljem $F$ in za vse $x,y\in A$ in $\lambda\in F$ velja: $\phi(x+y)=\phi(x)+\phi(y)$; $\phi(xy)=\phi(x)\phi(y)$; $\phi(\lambda x)=\lambda\phi(x)$; $\phi(1)=1$. (T) Če je $\phi: A\to A'$ homomorfizem grup, je $\phi(1)=1$ in $\phi(x^{-1})=\phi(x)^{-1}$ za vse $x\in A$. (T) Če je $\phi: A\to A'$ homomorfizem aditivnih grup, je $\phi(0)=0$ in $\phi(-x)=-\phi(x)$ za vse $x\in A$. (T) Če je $\phi: A\to A'$ homomorfizem kolobarjev in je element $x\in A$ obrnljiv, je obrnljiv tudi $\phi(x)$ in velja $\phi(x^{-1})=\phi(x)^{-1}$. (T) Slika homomorfizma grup/prostorov/kolobarjev/algeber je podgrupa/podprostor/podkolobar/podalgebra. (T) Homomorfizem $\phi: A\to A'$ je injektiven natanko tedaj, ko je njegovo jedro trivialno (vsebuje le enoto 1/0). (T) Kompozitum homomorfizmov je homomorfizem. (T) Inverzna preslikava izomorfizma je izomorfizem. (P) Množica vseh avtomofizmov $A$ je za operacijo komponiranja grupa. (D) Če obstaja izomorfizem iz $A$ v $A'$, sta $A$ in $A'$ izomorfna/-i $A\cong A'$. (T) Končno-razsežna vektorska prostora $V$ in $V'$ nad poljem $F$ sta izomorfna natanko tedaj, ko imata enako dimenzijo. (P) Netrivialen končno-razsežen vektorski prostor nad poljem $F$ je izomorfen prostoru $F^n$ za neki $n\in\mathbb{N}$. Če je v homomorfizmu $red(a)=k$, potem velja $\phi(a)^k=\phi(a^k)=\phi(1)=1$, od tod sledi $red(\phi(a))\mid red(a)$. (p) Notranji avtomofizem poljubne grupe $G$, za vsak $a\in G$, definiramo s preslikavo $\phi_a: G\to G$ s predpisom $\phi_a(x)=axa^{-1}$.

**Podgrupe edinke in kvocientne grupe**

(D) Za vsako podgrupo $N$ grupe $G$ je množica $aNa^{-1}=\{ana^{-1}\mid n\in\mathbb{N}\}$ podgrupa $G$, imenovana konjugirana podgrupa podgrupe $N$. (D) Če podgrupa $N$ grupe $G$ zagošča pogoju $aNa^{-1}\subseteq N$ za vsak $a\in G$, se imenunje (podgrupa) edinka: $N\triangleleft G$. Velja: $N\triangleleft G\Leftrightarrow N\leq G$ in $aNa^{-1}\subseteq N$ za vsak $a\in G$. (p) Trivialna podgrupa $\{1\}$ in cela grupa $G$ sta edinki vsake grupe $G$. Vsaka podgrupa v Abelovi grupi je edinka. Center $Z(G)$ vsake grupe $G$ je edinka. Netrivialna edinka – vsaka edinka različna od $\{1\}$; prava edinka – vsaka edinka različna od $G$. (D) Enostavna grupa je netrivialna grupa, ki nima pravih netrivialnih edink. (T) Za podgrupo $N$ grupe $G$ je ekvivalentno: 1) $N$ je edinka.; 2) $aN\subseteq Na$ za $\forall a\in G$.; 3) $aN=Na$ za $\forall a\in G$.; 4) $aNa^{-1}=N$ za $\forall a\in G$. Produkt podgrupe z edinko je podgrupa. Produkt edink je edinka.; $H\leq G, N\triangleleft G\Rightarrow HN=NH\leq G$.; $M,N\triangleleft G\Rightarrow MN=NM\triangleleft G$.; $M,N\triangleleft G\Rightarrow M\cap N\triangleleft G$. (I) Naj bo $N\triangleleft G$. Če v množico vseh odsekov $G/N$ vpeljemo množenje s predpisom $aN\cdot bN=(ab)N$, postane $G/N$ grupa. Preslikava $\pi: G\to G/N$, definirana s $\pi(a)=aN$, je epimorfizem in $\ker\pi=N$. (D) Grupi $G/N$ pravimo kvocientna grupa (tudi faktorska grupa), preslikavo $\pi$ imenujemo kanonični epimorfizem. (O) Če je $G$ aditivna grupa, operacijo v kvocientni grupi $G/N$ vpeljemo kot seštevanje $(a+N)+(b+N)=(a+b)+N$.; Množenje odsekov $aN\cdot bN=(ab)N$ je dobro definirano. (O) Če je $G$ končna grupa in $N$ njena poljubna edinka, je po Lagrangevem izreku $|G/N|=\frac{|G|}{|N|}$. (T) Podmnožica $N$ grupe $G$ je podgrupa edinka natanko tedaj, ko je $N$ jedro homomorfizma iz grupe $G$ v neko grupo $G'$. (I) Naj bo $U$ podprostor vektorskega prostora $V$. Če v množico vseh odsekov $V/U$ vpeljemo seštevanje in množenje s skalarji s predpisi $(v+U)+(w+U)=(v+w)+U$ in $\lambda(v+U)=\lambda v+U$, postane $V/U$ vektorski prostor. Preslikava $\pi: V\to V/U$, s predpisom $\pi(v)=v+U$ je epimorfizem in $\ker\pi=U$. (kvocientni vektorki prostor; kanonični epimorfizem)

**Ideali in kvocientni kolobarji**

(D) Naj bo $I$ podgrupa kolobarja $K$ za seštevanje. Če za vse $a\in K$ in $u\in I$ velja $au\in I$ in $ua\in I$, $I$ imenujemo ideal kolobarja $K$: $I\triangleleft K$. $I$ ideal kolobarja $K$: 1) $u-v\in I$ za $\forall u,v\in I$; 2) $KI\subseteq I$; 3) $IK\subseteq I$. ((1 in 2) - levi ideal; (1 in 3) - desni ideal) (p) $\{0\}$ in $K$ ideala kolobarja $K$. Glavni ideali: $aK=\{ax\mid x\in K\}$. $n\mathbb{Z}; n\in\mathbb{N}\cup\{0\}$ glavni ideali za $\mathbb{Z}$. (L) Če enostranski ali dvostranski ideal $I$ kolobarja $K$ vsebuje kak obrnljiv element, je enak celemu kolobarju $K$. (D) Vsota idealov $I$ in $J$ kolobarja $K$: $I+J=\{u+v\mid u\in I, v\in J\}$. Vsota je ideal. Produkt idealov $I$ in $J$ kolobarja $K$: $IJ=\{u_1v_1+\cdots+u_nv_n\mid u_i\in I, v_i\in J\}$. Produkt je ideal. Presek idealov $I$ in $J$ kolobarja $K$ je ideal kolobarja $K$. (I) Naj bo $I\triangleleft K$. Če v množico vsek odsekov $K/I$ vpeljemo seštevanje in množenje s predpisi $(a+I)+(b+I)=(a+b)+I$ in $(a+I)(b+I)=ab+I$, postane $K/I$ kolobar. Preslikava $\pi: K\to K/I$, s predpisom $\pi(a)=a+I$, je epimorfizem in $\ker\pi=I$. (kvocientni kolobar; kanonični epimorfizem) (O) Podgrupa za seštevanje $I$ kolobarja $K$ je ideal, ko je množenje odsekov $(a+I)(b+I)=ab+I$ dobro definirano. (T) Podmnožica $I$ kolobarja $K$ je ideal natanko tedaj, ko je $I$ jedro homomorfizma iz kolobarja $K$ v nek kolobar $K'$. (D) Ideal algebre definiran kot ideal kolobarja. Je podprostor, ker je za $\forall\lambda$ in $\forall u$ tudi $\lambda u=\lambda(1u)=(\lambda 1)u$ element ideala. (I) Naj bo $I$ ideal algebre $A$. Če v množico vseh odsekov $A/I$ vpeljemo seštevanje, množenje in množenje s sklarji s predpisi $(a+I)+(b+I)=(a+b)+I$, $(a+I)(b+I)=ab+I$ in $\lambda(a+I)=\lambda a+I$, postane $A/I$ algebra. Preslikava $\pi: A\to A/I$, s predpisom $\pi(a)=a+I$, je epimorfizem in $\ker\pi=I$. (kvocientna algebra, kanonični epimorfizem.)

**Izrek o izomorfizmu in primeri kvocientnih struktur**

(I - prvi izrek o izomorfizmu) Naj bo $\phi: A\to A'$ homomorfizem. Potem je $A/\ker\phi\cong\operatorname{Im}\phi$. (I) Vsaka ciklična grupa je izomorfna bodisi grupi $\mathbb{Z}$ bodisi grupi $\mathbb{Z}_n$ za nek $n\in\mathbb{N}$. (P) Netrivialna grupa $G$ nima pravih netrivialnih podgrup natanko tedaj, ko je $G$ ciklična grupa s praštevilskim redom (in je torej $G\cong\mathbb{Z}_p$ za nek $p\in\mathbb{P}$). (p) Velja: $G/\{1\}\cong G$ in $G/G\cong\{1\}$. $G/Z(G)\cong\operatorname{Inn}(G)$. ($\operatorname{Inn}(G)$ grupa notranjih avtomorfizmov). (O) Center $Z(G)$ vsake grupe $G$ je edinka, center $Z(K)$ nekomutativnega kolobarja $K$ ni ideal (vsebuje enoto 1). (D) Idealu $M$ kolobarja $K$ pravimo maksimalni ideal, če $M\neq K$ in če ne obstaja ideal $J$ z lastnostjo $M\subsetneq J\subsetneq K$. (I) Ideal $M$ komutativnega kolobarja $K$ je maksimalni ideal natanko tedaj, ko je kvocientni kolobar $K/M$ polje. (p) Velja: $K/\{0\}\cong K$ in $K/K\cong\{0\}$. (p) Za naravno število $p$ je ekvivalentno: 1) $p\in\mathbb{P}$; 2) Kolobar $\mathbb{Z}_p$ je polje.; 3) $p\mathbb{Z}$ je maksimalni ideal kolobarja $\mathbb{Z}$. (I - drugi izrek o izomorfizmu) Naj bo $G$ grupa, $H\leq G$ in $N\triangleleft G$. Velja: $H\cap N\triangleleft H$, $N\triangleleft HN$ in $H/(H\cap N)\cong HN/N$. (I - tretji izrek o izomorfizmu) Naj bo $G$ grupa, $M,N\triangleleft G$ in $N\subseteq M$. Velja: $G/M\cong(G/N)/(M/N)$.

**Korespondenčni izrek**

(L) Naj bo $\phi: G\to G'$ homomorfizem grup. 1) Če je $H'\leq G'$ je $\phi^{-1}(H')\leq G$.; 2) Če je $N'\triangleleft G'$ je $\phi^{-1}(N')\triangleleft G$.; 3) Če je $H\leq G$ je $\phi(H)\leq G'$.; 4) Če je $N\triangleleft G$ in je $\phi$ epimorfizem, je $\phi(N)\triangleleft G'$. (I - korespondenčni izrek) Naj bo $N\triangleleft G$. 1) Vsaka podgrupa grupe $G/N$ je oblike $H/N$ za neko podgrupo $H$ grupe $G$, ki vsebuje $N$.; 2) Vsaka podgrupa edinka grupe $G/N$ je oblike $M/N$ za neko podgrupo edinko $M$ grupe $G$, ki vsebuje $N$. (P) Vsaka podgrupa grupe $\mathbb{Z}_n$ je oblike $d\mathbb{Z}_n$, kjer $d\mid n$.