Algebra theory

C1:

- $r = (A, A, R)$ on A is called:

  (1) reflexive (r) : $\forall x \in A \ x r x$

  (2) transitive (t) : $x, y, z \in A \quad x r y$ and $y r z \Rightarrow x r z$

  (3) Symmetric (s): $x, y \in A \quad x r y \Rightarrow y r x$

  r equivalence relation if r has: $(r), (t), (s)$

- i) $r \in E(A) \quad A/r \in P(A)$

  ii) $\pi = (A_i)_{i \in I} \in P(A)$. $r_\pi \in E(A)$

  iii) $F: E(A) \to P(A)$ be def by: $F(r) = A/r \quad \forall r \in E(A)$

  $\Rightarrow F$ a bij. whose inverse is $G: P(A) \to E(A): G(\pi) = r_\pi \quad \forall \pi \in P(A)$

  A/r - partition corresponding to r.

C2:

- Let "·" be an operation on A:

  (1) Associative law: $(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall x, y, z \in A$

  (2) Commutative law: $x \cdot y = y \cdot x \quad \forall x, y \in A$

  (3) Identity law: $\exists e \in A$ s.t $\forall a \in A \quad a \cdot e = e \cdot a = a$ (e - identity element)

  (4) Inverse law: $\forall a \in A \ \exists a'$ s.t $a \cdot a' = a' \cdot a = e$

- "·" op on A:

  (i) If $\exists e \Rightarrow$ it is unique

  (ii) If $\exists x' \Rightarrow$ it is unique

- stable subset: $\varphi: A \times A \to A \quad B \subseteq A$, B stable subset if: $\forall x, y \in B \ \varphi(x, y) \in B$

- $(A, \cdot)$ called: (1) semigroup if ~~it is~~ asoc. law holds

  (2) monoid if: semigroup with id.el

  (3) group if it is a monoid $\forall x \in A$ is inversable.

  (4) abelian group if it is comutative group

• R a set : $(R,+,\cdot)$: (1) ring if $(R,+)$ is abelian group, $(R,\cdot)$ semigroup and distributive law holds:

$$x\cdot(y+z) = x\cdot y + x\cdot z \quad \forall x,y,z\in R$$
$$(y+z)\cdot x = yx + zx \quad \forall x,y,z\in R$$

(2) unitary ring $\exists e$

(3) division ring: $(R,+)$ abel gr $(R^*,\cdot)$ gr. dist. law

(4) field: commutative division ring

$(R,+,\cdot)$ comut if the op "$\cdot$" comut

• $H\subseteq G$ H subgroup if: (1) H stable subset
$(G,\cdot)$ - gr
(2) $(H,\cdot)$ is a group

• $(G,\cdot)$ $(G'',\cdot)$ groups $f: G\to G'$ f group homomorph:

$$f(x\cdot y) = f(x)\cdot f(y) \ \forall x,y\in G$$

f - bij => isomorphism.

• f gr homomorph => $f(1)=1'$; $(f(x))^{-1} = f(x^{-1})$

C3:

- A vector space over K is an abelian group $(V,+)$

$$\cdot : K\times V \to V \quad , (k,v)\mapsto kv$$

satisfying :

(1) $k\cdot(v_1+v_2)=k\cdot v_1+k\cdot v_2$

(2) $(k_1+k_2)\cdot v = k_1\cdot v+k_2\cdot v$

(3) $(k_1\cdot k_2)\cdot v = k_1\cdot(k_2\cdot v)$

(4) $1\cdot v=v$.

- Let V v.s over K $\quad S\subseteq V$, S subspace of V if:

(1) $S\neq\emptyset$

(2) $\forall v_1,v_2\in S \Rightarrow v_1+v_2\in S$

(3) $\forall k\in K\ \forall v\in S\ \ k\cdot v\in S$

C4:

- V v.s $\quad X\subseteq V$:

$$\langle X\rangle = \cap\{S\leq V \mid X\subseteq S\}$$

we call it the subspace generated by X

- V v.s over K

finitely generated if $\exists v_1 \dots v_m\in V\ (m\in\mathbb{N})$ s.t $V=\langle v_1\dots v_m\rangle$

- V v.s over K

$$k_1v_1+\dots+k_mv_m$$

is called a linear combination of the vectors $v_1,\dots,v_m$

- V v.s over K $\quad x_1\dots x_m\in V$

$$\langle x_1\dots x_m\rangle = \{k_1x_1+\dots+k_mx_m \mid k_i\in K\}$$

- V v.s over K $\quad S,T\leq V$

$$S+T=\{s+t \mid s\in S;\ t\in T\}$$

if $S\cap T=\{0\}$ $\quad S+T$ is denoted by $S\oplus T$

- $S+T=\langle S\cup T\rangle$

• V v.s K $S, T \leq V \Rightarrow S+T \leq V$

• Let V, V' v.s over the field K

$f: V \to V'$ is: (1) (K-) linear map (homomorphism or linear trans.) if:

$$f(k_1 v_1 + k_2 v_2) = k_1 f(v_1) + k_2 f(v_2) \iff \begin{cases} f(v_1+v_2) = f(v_1) + f(v_2) & \forall v_1, v_2 \in V \\ f(kv) = k f(v) & \forall k \in K \ \forall v \in V \end{cases}$$

(2) isomorphism if bij

(3) endomorphism if K lm $\Rightarrow V = V'$

(4) automorphism if bij and $V = V'$

• $f: V \to V'$: $\operatorname{Ker} f = \{ v \in V \mid f(v) = 0' \}$

$\operatorname{Im} f = \{ f(v) \mid v \in V \}$

• $\operatorname{Ker} f \leq V$

$\operatorname{im} f \leq V'$

• $f: V \to V'$ $\Rightarrow \operatorname{Ker} f = \{0\} \iff f$ inj

• V and V' v.s over K

$\operatorname{Hom}_K(V, V')$: $\forall f, g \in \operatorname{Hom}_K(V,V')$ $\forall k \in K$ $f+g,\ k \cdot f \in \operatorname{Hom}_K(V, V')$

$$\left.\begin{aligned} (f+g)(v) &= f(v) + g(v) \\ (kf)(v) &= k f(v) \end{aligned} \quad \forall v \in V \right\} \Rightarrow \operatorname{Hom}_K(V, V') \text{ v.s over } K$$

• V v.s over K $\Rightarrow \operatorname{End}_K(V)$ v.s over K

C5.

- V v.s over K $\quad v_1 .. v_n \in V$

(1) liniarly independent $\forall k_i \in K$

$$k_1 v_1 + .. + k_n v_n = 0 \Rightarrow k_1 = .. = k_n = 0$$

- V v.s over K . $B = (v_1 .. v_n) \in V^n$ is a basis of V if:

(1) B liniarly independent in V.

(2) B is a syst of generators for V, $\langle B \rangle = V$

$\forall$ v.s has a base

- V v.s over K $\quad B = (v_1 .. v_n)$ basis if $\forall v \in V$ can be uniquely written as a linear cambimation:

$$v = k_1 v_1 + .. k_n v_n$$

- $B = (v_1 .. v_n)$ basis of V and $v \in V$ Then $k_1 .. k_n \in K$ from the linear $v = k_1 v_1 + .. k_n v_n$ of vectors B are the coordinates of v in B

C6

- Any 2 bases of v.s have the same nr of el
- V v.s over K. The nr of el is called the $\dim_K V$ or $\dim V$
- The max nr of linearly independent vector in V is $\dim V = n$
- The min nr of generators for V is $\dim V = n$
- X lin indep in $V \Leftrightarrow X$ is a syst of generators for V
- $\forall$ linearly independent list of vectors in v.s can be completed to a basis of v.s

- V v.s over K $\quad S \leq V$:

(1) $\forall$ basis of S is part of a basis of V

(2) $\dim S \leq \dim V$

(3) $\dim S = \dim V \Leftrightarrow S = V$

- V v.s over K $S \leq V$. Subspace $\bar{S}$ of V s.t $V = S \oplus \bar{S}$ is called a complement of S in V

- $V \simeq V' \iff \dim V = \dim V'$
- $\dim V = n$ is isomorphic to the canonical vector space K^n over K
- $\dim(\ker f)$ the nullity of f and is denoted by $null(f)$.
- $\dim(\mathrm{Im} f)$ the rank of f denoted by $rank(f)$
- $\dim V = \dim(\ker f) + \dim(\mathrm{Im} f)$
- $\dim S + \dim T = \dim(S \cap T) + \dim(S+T)$
- $V = S \oplus T$: $\dim V = \dim S + \dim T$