Algebra I

(Algebra 0 + algebr. Geometry) (2,3) (+ Kom. Stochastik / distr. Geometrie)

- Atiyah–Macdonald: Comm. Algebra
- Eisenbud: C.A. (towards alg. geometry)

① Rings, ideals, modules ...

Def: R = ring $\rightsquigarrow$ "commutative ring with $1 = 1_R$"

(i.e. $(R, +, \cdot)$ $+, \cdot : R \times R \to R$ $(0_R \in R)$

axioms:
- $(R, +)$ = abelian group
- $\cdot$ is associative, commutative, $\exists\, 1_R : r \cdot 1 = 1 \cdot r = r$
  (we do not ask for the existence of r^{-1} in R)
- distributive: $\forall a, b, c \in R: \; a \cdot (b + c) = ab + ac$.

Exple: $\mathbb{Z}$, fields $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ (p = prime)

Def: R = ring $\rightsquigarrow$ $R^* = \{ r \in R \mid \exists\, s \in R : r \cdot s = 1_R \}$ "units of R".

$\rightsquigarrow (R^*, \cdot)$ – group. • **Ex:** R = field $\iff R^* = R \setminus \{0\}$

$r \in R^*$ $\rightsquigarrow$ s of the def. above is unique, and $s =: r^{-1}$ $\quad (r \in R \rightsquigarrow \exists\, r^{-1} \in R \;(?))$

• **Ex:** $\mathbb{Z}^* = \{1, -1\}$; $(\mathbb{Z}/n\mathbb{Z})^* = \{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1 \}$

Special case: $n = p$ = prime number $\rightsquigarrow (\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\} \rightsquigarrow$ field ($\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$)

∃ bad things: **Def:**
- $r \in R$ is a "zero-divisor" $\iff$ $\exists\, s \in R \setminus \{0\} : r \cdot s = 0$, $r \neq 0$
- R = "integral domain" $\iff$ R = ring without zero-divisors.

Exple: $R = \mathbb{Z}/6\mathbb{Z}$; $2 \cdot 3 = 0$ in R (not a domain)

Remark: $r \in R^* \implies r$ not zero divisor:

Proof: ↳ $\exists\, r^{-1} \in R$; if r = zero-div $\implies \exists\, s : rs = 0 \implies s = 1 \cdot s = (r^{-1} \cdot r)\, s = r^{-1}(rs) = r^{-1} \cdot 0 = 0$

Def: $r \in R$ called "nilpotent" $\iff \exists\, k \in \mathbb{N}_{\geq 1} : r^k = 0$ in R.

Remark: $r \neq 0$, nilpotent $\rightsquigarrow$ r = 0-divisor: k_0 = min k with $r^k = 0 \geq 2$.
$\implies 0 = r^k = r \cdot r^{(k-1)}$ and $s \neq 0$.

Exple: $R = \mathbb{Z}/9\mathbb{Z} \rightsquigarrow 3^2 = 0$ in R

Def: M = "R-module" (R = fixed ring) $\iff$ • $(M, +)$ = abelian group
• $\exists$ $R \times M \to M$, $(r, m) \mapsto r \cdot m$

such that:
- $\forall r, s \in R, m \in M$: $(r \cdot s) \cdot m = r \cdot (s \cdot m)$
- $1_R \cdot m = m$ (; $0_R \cdot m = 0_M$ $\quad (0 \cdot m = 0)$; $r \cdot 0_M = 0_M$)
- $r, s \in R$, $m, n \in M$: $(r + s) \cdot m = rm + sm$; $r \cdot (m + n) = r \cdot m + r \cdot n$.

Ex: (0) R = field $K \implies$ [K-modules = K-Vector spaces] (e.g. $K^2, K^3, \ldots$)

(1) $R = \mathbb{Z} \implies$ possible $\mathbb{Z}$-modules: $\mathbb{Z}$, $\mathbb{Z}^2$, $\mathbb{Z}/n\mathbb{Z}$ (e.g. $3 \cdot \bar{4} = \bar{12} = \bar{0}$ in $\mathbb{Z}/12\mathbb{Z}$; $3 \in \mathbb{Z}$, $\bar{4} \in \mathbb{Z}/12\mathbb{Z}$; torsion element)

Def:
- $m_1, \ldots, m_k \in M$ are linearly indep $\iff$ every LK $\sum_i r_i m_i = 0$ $(r_i \in R)$ forces $r_1 = \ldots = r_k = 0$.
- $m_1, \ldots, m_k \in M$ generate M $\iff \forall m \in M \; \exists\, r_i \in R : m = \sum r_i m_i$. ($\mathbb{Z}$, M: $6 \cdot m = 0_M$)

Ex-ple: $\mathbb{Z}/6\mathbb{Z}$ ($= M$) has no basis: Every $m \in \mathbb{Z}/6\mathbb{Z}$ is lin. dependent.

Def. $N \subseteq M$ is a sub module $\iff$ N, M = R-modules, s.t. $R \times N \to N$ is the restriction of $R \times M \to M$

Ex. (0) R is an R-module. $\rightsquigarrow \forall k \geq 1 : R^k = R$-module ("the free R-module of rank k")

(1) submodules of R are called "ideals" of R. , e.g. $9 \cdot \mathbb{Z} \subseteq \mathbb{Z}$ or $n \cdot \mathbb{Z} \subseteq \mathbb{Z}$ (for $n \in \mathbb{Z}$)

Def R, S = rings; $f: R \to S$ is called a (ring-) homomorphism (for all $a, s \in R$) $\iff$ $f(a+s) = f(a) + f(s)$, $f(as) = f(a) \cdot f(s)$, $f(1_R) = 1_S$

Exmple: Let $f: R \to S$ a ring homomorphism (e.g. ① $\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ or ② $\mathbb{Z} \hookrightarrow \mathbb{Q}$, ③ $\mathbb{Q} \hookrightarrow R$)

Then: S becomes an R-module: $R \times S \to S$, $(r, s) \mapsto r \cdot s := f(r) \cdot s$ ("S is an R-algebra" (better than just an R-module))

e.g.: ① $\mathbb{Z}/6\mathbb{Z}$ becomes a $\mathbb{Z}$-algebra (= $\mathbb{Z}$-module)
② $\mathbb{Q}$ "is" a $\mathbb{Z}$-algebra
③ $\mathbb{R}$ is a $\mathbb{Q}$-algebra

} generalizes to: Every ring S is (in a natural way) a $\mathbb{Z}$-algebra, namely: $\mathbb{Z} \to S$, $1 \mapsto 1_S$, $n \in \mathbb{N} \mapsto \underbrace{1_S + \dots + 1_S}_{n\text{-times}}$

Thm: If $f: M \to L$ is a R-linear map, i.e.: R-module homomorphism (i.e. for $r \in R$, $m, n \in M$: $\cdot f(m+n) = f(m) + f(n)$, $\cdot f(rm) = r f(m)$)
$\Rightarrow$
- $\ker f$ is an R-submodule of M
- $\operatorname{im} f$ is an R-submodule of L
- $M/\ker f \xrightarrow{\sim} \operatorname{im} f$.

Special case: R = ring $\rightsquigarrow$ R-module over R; $I \subseteq R$ ideal (i.e. submodule of R) $\Rightarrow$ R/I = R-module, $\pi: R \to R/I$ R-linear

Recall: R/I = ring; $\pi: R \to R/I$ ring homomorphism

$\bar{r}, \bar{s} \in R/I$ ($= r+I$, $= s+I$) $\rightsquigarrow \bar{r} \cdot \bar{s} := \overline{rs}$, i.e. $(r+I)\cdot(s+I) := rs+I$

Check: does not depend on repr.: $r' \in r+I \Rightarrow r's+I = rs+I$, i.e. $(r'-r)s = r's - rs \in I$ (follows from $s \in R, q \in I \Rightarrow sq \in I$)

e.g.: $\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$

V/U : G/N Sticky: M = R-module, U, N = R-submodule $\Rightarrow$ M/N = R-module: $\pi: M \to M/N$

$M/N = \{g \cdot N \mid g \in G\} = \{m+N \mid m \in M\}$

- abelian grp with $+$ (ok)
- $r \in R$, $m+N \in M/N$: $r \cdot (m+N) := (rm)+N$

(need to show: $m+N = m'+N \Rightarrow (rm)+N = (rm')+N$)

Exmple: K field, $K[x]$:= polynomial ring $= \{\sum_{i=0}^{n} a_i x^i \mid a_i \in K, n \in \mathbb{N}\}$, x = formal symbol
R = ring, $R[x]$ " " $= \{$ " " $\mid a_i \in R \dots\}$

$x^i \cdot x^j := x^{i+j}$

e.g.: $(1+2x^2)\cdot(x-1) = 1\cdot x - 1\cdot 1 + 2x^2 \cdot x - 2x^2 \cdot 1 = x - 1 + 2x^3 - 2x^2$
$= (1 \cdot x^0 + 0 \cdot x^1 + 2 \cdot x^2)\cdot(1 \cdot x^1 - 1 \cdot x^0)$

$f \in R[x]$, $f = \sum_{i=0}^{n} c_i x^i$, $c_n \neq 0$ $\rightsquigarrow$ $n =: \deg(f)$; $\deg 0 := -\infty$

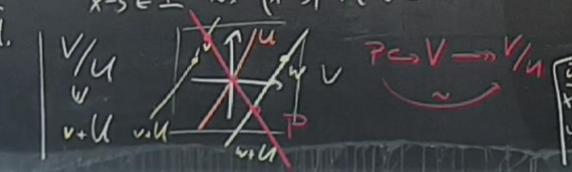
$R \hookrightarrow R[x]$, $r \mapsto r \cdot x^0 = r$

Remark: R = domain $\Rightarrow \deg(f \cdot g) = \deg f + \deg g$.
$\deg(f+g) \leq \max\{\deg f, \deg g\}$

Ideals in $K[x]$: $(x-3) := (x-3)\cdot K[x]$ (want a ideal $I \subseteq K[x]$ with $x-3 \in I \rightsquigarrow (x-3)\cdot K[x] \subseteq I$)

$K[x]/(x-3)$ = quotient ring, ideal.

$f(x) + (x-3)\cdot K[x]$



$K[x]/(x-3)$: we need a ring homom. $f: K[x] \to K$, $\ker f = (x-3)$

try: $f: K[x] \to K$, $(c \in K) \mapsto c$, $x \mapsto 3$; $g(x) \mapsto g(3)$

$K[x]/(x-3)$: $x-3 \mapsto 0$, $1 \rightsquigarrow 3 \mapsto 3$, $x \mapsto 3$, $\ker f = (x-3)$

provides: $K[x]/(x-3) \xrightarrow{\sim} K$, $x \mapsto 3$

$K[x,y] := K[x][y] = \{\sum_{i,j=0}^{n} a_{ij} \cdot x^i y^j \mid a_{ij} \in K\}$ $(x^i y^j)\cdot(x^a \cdot y^b) := x^{a+i} \cdot y^{b+j}$

$I := (y^2 - x^3)\cdot K[x,y]$ ideal in $K[x,y]$; Q: what "is" $K[x,y]/(y^2-x^3)$? (OK / NOT)

e.g.: $K[x,y] \to K[t]$, $x \mapsto t^2$, $y \mapsto t^3$

want: $\ker f = (y^2 - x^3)\cdot K[x,y]$

more precisely: $y^2 - x^3 \in \ker f$, i.e.: $f(y^2) = f(x^3)$, i.e.: $f(y)^2 = f(x)^3$.

$K[x,y]/(y^2-x^3) \xrightarrow{\text{OK}} K[t^2, t^3] = \{f(t) \in K[t] \mid t^1\text{-coeff vanishes}\}$.

$\mathbb{R}[x,y] \xrightarrow{f} \mathbb{R}[t]$, $x \longmapsto t^2$, $y \longmapsto t^3$

Claim: $\ker f = (y^2 - x^3) \cdot \mathbb{R}[x,y]$ (= I)

we have seen: $x^3 \mapsto t^6 \longleftarrow y^2 \Rightarrow y^2 - x^3 \in \ker f$

$\Rightarrow (y^2-x^3)\cdot\mathbb{R}[x,y] \subseteq \ker f$.

Let $p(x,y) \in \ker f \subseteq \mathbb{R}[x,y] \rightsquigarrow p(x,y) = \sum_{i=0}^{n} a_i(x)\cdot y^i$ $\rightsquigarrow$ If y^2 appears in $p(x,y)$, we can substitute it by x^3!

i.e.: if $g(x,y)\cdot y^2$ appears in $p(x,y)$ (ex: $\underbrace{(x+x^7)\cdot y^{10}}_{g(x,y)}\cdot y^2$)

$\Downarrow$ substitute by $g(x,y)\cdot x^3$, i.e.: this really means to add $g(x,y)\cdot(x^3-y^2) \in I$

$\Rightarrow$ We can reduce $p(x,y)$ via elements of I to lower the powers of y!

i.e.: $\exists\ r(x,y) \in I$: $q(x,y) := p(x,y) - r(x,y)$ has a lower y-power

$q(x,y) \in \ker f$ ($\Leftarrow$), $r(x,y) \in I \subseteq \ker f$ known

v.l.o.s: $q(x,y) = a(x) + y\cdot s(x)$ $\rightsquigarrow$ remains to show: $q(x,y) \in I$.

Restart: Let $q(x,y) = a(x) + y\cdot s(x) \in \ker f$; show: $q(x,y) \in I$.

$a(x) = \sum a_i x^i$, $s(x) = \sum s_i x^i$

$f(a(x) + y\,s(x)) = 0$

$f(a(x)) + f(y)\cdot f(s(x)) = \underbrace{a(t^2)}_{\text{monomials } t^{2\cdot}} + \underbrace{t^3\cdot s(t^2)}_{\text{monomials } t^{2\cdot+1}} = 0$

$\Rightarrow a(t^2) = 0$, $t^3\cdot s(t^2) = 0$

$a(t^2) = s(t^2) = 0 \rightsquigarrow a(x) = s(x) = 0 \Rightarrow q(x,y) = 0$ //

Properties / Facts of ideals in rings — Let $I, J \subseteq R$ be ideals.

- $0 \in I$ ($R\cdot I \subseteq I$, $I + I \subseteq I$; $0\cdot I \in I$)
- $[1 \in I] \Leftarrow [I = R]$

smallest ideal: $\{0\} = (0)$

largest: $R = (1)$

- $a_1, \dots, a_n \in R \rightsquigarrow (a_1, \dots, a_n) :=$ smallest ideal $I \subseteq R$ containing $a_1, \dots, a_n$ ("generated by $a_1, \dots, a_n$")
  $= a_1\cdot R + a_2\cdot R + \dots + a_n\cdot R$

Ex-ple: $\cdot\ (x-3) \subseteq \mathbb{R}[x]$ is $(x-3)\cdot\mathbb{R}[x]$

$\cdot\ (x,y) \subseteq \mathbb{R}[x,y]$ is $x\,\mathbb{R}[x,y] + y\,\mathbb{R}[x,y] = \{f(x,y) \in \mathbb{R}[x,y] \mid f(0,0) = 0\}$

$R = \mathbb{Z}$ $\rightsquigarrow$ $(3) = 3\cdot\mathbb{Z}$; $(3,5) = 3\cdot\mathbb{Z} + 5\cdot\mathbb{Z} \ni 1 \Rightarrow (3,5) = (1) = \mathbb{Z}$.

$\llcorner\ \exists\ k,l \in \mathbb{Z}:\ 3\cdot k + 5\cdot l = \gcd(3,5) = 1$ ⌋

- $r \in R$ $\rightsquigarrow$ ideal (r) = ideal generated by 1 element (usually r) $\rightsquigarrow$ "principal ideal"
- $I, J \subseteq R$ ideals $\rightsquigarrow$ $I + J := \{a+b \mid a \in I, b \in J\}$ e.g.: $(3,5) = (3) + (5)$

  $I = (a_1, \dots, a_n)$; $J = (b_1, \dots, b_\ell)$ $\rightsquigarrow$ $I + J = (a_1, \dots, a_n, b_1, \dots, b_\ell)$
- $I \cap J$ = ideal in R! $I \cup J$ is almost never an ideal.

  $(I \cup J) := [\text{ideal generated by } I \cup J] = I + J$.

$I \cdot J := (\{ab \mid a \in I, b \in J\}) = \{\sum_{i=0}^{\ell} a_i b_i \mid a_i \in I, b_i \in J\}$: If $I = (a_1, \dots, a_n)$, $J = (b_1, \dots, b_\ell)$

$\Rightarrow I J = (a_i b_j \mid \substack{i=1,\dots,n \\ j=1,\dots,\ell})$

Radical: $I \subseteq R$ $\rightsquigarrow$ $\sqrt{I} := \{r \in R \mid \exists\ k \geq 1 : r^k \in I\}$ is an ideal.

Proof:

- $r \in \sqrt{I}$, $s \in R$ $\overset{(?!)}{\rightsquigarrow}$ $sr \in \sqrt{I}$

  $\Downarrow$

  $\exists\ k : r^k \in I$ $\rightsquigarrow$ $r^k\cdot s^k \in I$ $\rightsquigarrow$ $rs \in \sqrt{I}$

  $= (rs)^k$
- $r, s \in \sqrt{I}$; show: $r + s \in \sqrt{I}$

  $\exists k, \ell \geq 1 : r^k, s^\ell \in I$ $\rightsquigarrow$ $(r+s)^{k+\ell-1} = \sum_{\nu=0}^{k+\ell-1} \binom{k+\ell-1}{\nu} r^\nu s^{k+\ell-1-\nu}$

  either $\nu \geq k$ or $\mu \geq \ell$ (otherwise $\nu \leq k-1$, $\mu \leq \ell-1$)

  $k+\ell-1 = \mu+\nu \leq k+\ell-2$ ↯

$f : R \to S$ ring homomorphism. $I \subseteq R$, $J \subseteq S$ ideals

- $f(I) \subseteq S$ is in general not an ideal! (ex: $\mathbb{Z} \hookrightarrow \mathbb{Q}$)

  $\rightsquigarrow$ instead: consider $(f(I)) := f(I)\cdot S$ ($I = \mathbb{Z} \rightsquigarrow (I) = \mathbb{Z} \subset \mathbb{Q}$ not ideal)

  (except: If f = surjective $\rightsquigarrow$ $f(I) = f(I)\cdot S$, i.e. it is already an ideal)
- $f^{-1}(J) \subseteq R$ is an ideal. Even: $R/f^{-1}(J) \hookrightarrow S/J$ Special case: $J = (0)$ $\Rightarrow f^{-1}(0) = \ker f$