Seminar 2

The residue class ring modulo n

Let $n \in \mathbb{N}$, $n \geq 2$.

$\underline{\underline{T}}$ (The Division Algorithm for integers):

$\forall a, b \in \mathbb{Z}$, $b \neq 0$, $\exists! \, q, r \in \mathbb{Z}$: $a = bq + r$, with $0 \leq r < |b|$.

$\hat{0} = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$

$\hat{1} = 1 + n\mathbb{Z} = \{1 + nk \mid k \in \mathbb{Z}\}$ $\qquad \mathbb{Z}_n = \{\hat{0}, \hat{1}, \dots, \widehat{n-1}\}$

$\vdots$

$\widehat{n-1} = (n-1) + n\mathbb{Z} = \{(n-1) + nk \mid k \in \mathbb{Z}\}$

$$\hat{i} + \hat{j} = \widehat{i+j}, \quad \hat{i} \cdot \hat{j} = \widehat{ij}$$

$(\mathbb{Z}_n, +)$ Abelian group

assoc., comm., $\hat{0}$ additive identity elem.

$\hat{a} \in \mathbb{Z}_n$, $-\hat{a} = \widehat{-a} \; (= \widehat{n-a})$

$(\mathbb{Z}_n, \cdot)$ comm. monoid.

assoc., comm., $\hat{1}$ multipl. id. elem.

„$\cdot$" distr. w.r.t. „$+$"

$\Longrightarrow (\mathbb{Z}_n, +, \cdot)$ comm. unitary ring, $\hat{0} \neq \hat{1}$.

$n = 4$, $(\mathbb{Z}_4, +, \cdot)$ has zero divisors.

$$\hat{2} \neq \hat{0}, \quad \hat{2} \cdot \hat{2} = \hat{4} = \hat{0}$$

$n = 2$, $(\mathbb{Z}_2 = \{\hat{0}, \hat{1}\}, +, \cdot)$ field.

$\underline{\underline{Ex}}$: Let $n \in \mathbb{N}$, $n \geq 2$, $\hat{a} \in \mathbb{Z}_n$. Show that

$\hat{a}$ is a unit in $\mathbb{Z}_n \iff (a, n) = 1$. ($a, n$ coprime).

$\underline{\underline{Solution}}$: Remind that:

$a, b \in \mathbb{Z}$, $\hat{a} = \hat{b} \iff n \mid a - b$ ✓

$(a, b) = 1 \iff \exists \, p, q \in \mathbb{Z} : \underline{p} a + \underline{q} b = 1$.

„$\Longrightarrow$" $\hat{a}$ is a unit in $\mathbb{Z}_n \iff \exists \, \hat{c} \in \mathbb{Z}_n$: $\hat{a} \cdot \hat{c} = \hat{1}$

$\hat{1} = \hat{a} \cdot \hat{c} = \widehat{ac} \iff n \mid ac - 1 \iff \exists k \in \mathbb{Z} : \underline{ac - 1 = nk}$.

$\Longrightarrow \exists \, c, k \in \mathbb{Z}$: $\underline{c}a + (\underline{-k})n = 1 \Longrightarrow (a, n) = 1$.

„$\Longleftarrow$" Let us consider that $(a, n) = 1 \iff \exists \, p, q \in \mathbb{Z} : pa + qn = 1$

$\Longrightarrow \hat{1} = \widehat{pa + qn} = \widehat{pa} + \underbrace{\widehat{qn}}_{= \hat{0}} = \widehat{pa} = \hat{p} \cdot \hat{a}$

$\Longrightarrow \hat{a}$ is a unit in $\mathbb{Z}_n$ and $\hat{a}^{-1} = \hat{p}$.

C: $(\mathbb{Z}_n,+,\cdot)$ is a field $\Leftrightarrow$ n is a prime $(n\in\mathbb{N}, n\geq 2)$.

proof: $\mathbb{Z}_n$ field $\Leftrightarrow$ $\hat{1},\dots,\widehat{n-1}$ are units $\Leftrightarrow$

$\Leftrightarrow (1,n)=(2,n)=\dots=(n-1,n)=1 \Leftrightarrow$ $1, n$ are the only natural divisors of n

$\Leftrightarrow$ n is a prime.

Polynomial rings

Let $(R,+,\cdot)$ be a comm. unitary ring,

$R[X]=\{f=a_0+a_1X+\dots+a_nX^n \,/\, a_0,a_1,\dots,a_n\in R,\ n\in\mathbb{N}\}$
the set of polynomials over R.

$f,g\in R[X]$, $f=a_0+a_1X+\dots+a_nX^n$, $g=b_0+b_1X+\dots+b_nX^n$, $f+g=(a_0+b_0)+(a_1+b_1)X+\dots+(a_n+b_n)X^n$

$f=\underline{a_0}+\underline{\underline{a_1}}X+\dots+a_nX^n$, $g=\underline{b_0}+\underline{\underline{b_1}}X+\dots+b_mX^m$

$fg=c_0+c_1X+c_2X^2+\dots+c_{m+n}X^{m+n}$

$$\begin{cases} c_0=a_0b_0\\ c_1=a_0b_1+a_1b_0\\ c_2=a_0b_2+a_1b_1+a_2b_0\\ \vdots\\ c_{m+n-1}=a_{n-1}b_m+a_nb_{m-1}\\ c_{m+n}=a_nb_m\end{cases}$$

$(R[X],+,\cdot)$ comm. unitary ring.

"$\cdot$" is distr. w.r.t. "+"

$(R[X],+)$ Abelian group : zero elem = zero polynomial $0\,(\in R)$

$(R[X],\cdot)$ comm. monoid : the multipl. id. elem. $1\,(\in R)$

$\forall f\in R[X], f\neq 0$, f can be uniquely written as

$f=a_0+a_1X+\dots+a_nX^n$, $a_0,\dots,a_n\in R$, $a_n\neq 0$ (1)

$$\deg f=\begin{cases}-\infty, & f=0\\ n, & \text{if } f\neq 0 \text{ is given by (1)}\end{cases}$$

$\deg f=0 \Leftrightarrow f=a_0\neq 0 \Leftrightarrow a\in R\setminus\{0\}$

Remarks: 1) $\deg(f+g)\leq \max\{\deg f, \deg g\}$

2) $\deg(fg)\leq \deg f+\deg g$

Ex: $\mathbb{Z}_4[X]\ni f,g$

$f=\hat{2}X^2,\ g=\hat{2}X+\hat{1}\ ,\ fg=\underbrace{\hat{4}}_{=\hat{0}}X^3+\hat{2}X^2=\hat{2}X^2$

$\deg(fg)=2\neq 2+1=\deg f+\deg g$

3) R integral domain $\Longrightarrow \deg(fg)=\deg f+\deg g$

4) R field $\Longrightarrow \deg(fg)=\deg f+\deg g$

<u>Ex</u>: Show that: K field $\overset{?}{\Longrightarrow} K[X]$ integral domain

<u>Solution</u>: $0\neq 1 \Rightarrow K[X]$ comm. unital ring, $0\neq 1$ with no zero divisors (?)

$f,g\in K[X],\ fg=0 \overset{?}{\Longrightarrow} f=0$ or $g=0$

$\underline{fg=0} \Longrightarrow -\infty=\deg 0=\deg(fg)=\deg f+\deg g$

$\Longrightarrow \deg f=-\infty$ or $\deg g=-\infty \Longrightarrow \underline{f=0 \text{ or } g=0}$

<u>Ex</u>: Let K be a field. Show that $f\in K[X]$ is a unit $\Longleftrightarrow f\in K^*(=K\setminus\{0\})$.

<u>Solution</u>: „$\Longleftarrow$" Obviously.

„$\Longrightarrow$" $f\in K[X]$ unit $\Longrightarrow \exists\, g\in K[X]: fg=1$.

$\Longrightarrow \underline{0}=\deg 1=\deg(fg)=\underline{\deg f+\deg g} \Longrightarrow \deg f=\deg g=0 \Longrightarrow f\in K^*$

<u>Rings of square matrices over fields</u>

Let $(R,+,\cdot)$ be a comm. ring unitary, $m,n\in\mathbb{N}^*$ (1 the multipl. id. elem. of R)

$\left\{\begin{array}{l} A:\{1,\dots,m\}\times\{1,\dots,n\}\to R\ ,\quad A(i,j)=a_{ij}\in R \\ \text{an } m\times n \text{ matrix over } R\end{array}\right.$

$$A=\left(\ \cdots\ a_{ij}\ \cdots\ \right)=(a_{ij})$$

$A=(a_{ij}),\ B=(b_{ij}),\ A,B\in M_{m,n}(R)$

$A+B=(a_{ij}+b_{ij})\in M_{m,n}(R)$

$\left\{\begin{array}{l} +: M_{m,n}(R)\times M_{m,n}(R)\to M_{m,n}(R) \\ \text{assoc, comm.}\end{array}\right.$

$$O_{m,n}=\begin{pmatrix}0&\cdots&0\\ \vdots&&\vdots\\ 0&\cdots&0\end{pmatrix}$$ additive identity elem. (zero matrix)

$-A=(-a_{ij})\in M_{mn}(R)$

$(M_{m,n}(R),+)$ Abelian group.

$A=(a_{ij})\in M_{m,n}(R),\ B=(b_{ij})\in M_{n,p}(R)$

$AB=(c_{ij})\in M_{m,p}(R)$

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj} \in R$$

$\cdot : M_{m,n}(R) \times M_{n,p}(R) \to M_{m,p}(R)$ $\Big|$ $\Longrightarrow$ $\cdot : M_n(R) \times M_n(R) \to M_n(R)$

$m = n = p$

$(M_n(R), +)$ Abelian group

$(M_n(R), \cdot)$ monoid

- assoc.

„ $\cdot$ " is distr. w.r.t. „ $+$ " (both sides)

the multipl. id. elem.

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ - & - & - & - \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

$\Bigg\}$ $(M_n(R), +, \cdot)$ is a unitary ring

<u>Ex</u>: If $n \geq 2$, the ring $(M_n(R), +, \cdot)$ is a <u>non-comm.</u> ring which has zero-divisors.

Homework.

<u>Ex</u>: $(M_2(\mathbb{R}), +, \cdot)$ is non-comm. and has zero divisors.

<u>Solution</u>: Let us consider $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ are zero divisors

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\neq$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

<u>Remark</u>: Let $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$

$\forall a, b \in \mathbb{R}$, $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \Longrightarrow A$ is closed in $(M_2(\mathbb{R}), \cdot)$

$(A, \cdot)$ monoid comm.

ind. op.

assoc., comm.

$\cancel{I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \notin A$

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is the identity elem. of $(A, \cdot)$.

Let $n \in \mathbb{N}^*$, K field. , $(M_n(K), +, \cdot)$ unitary ring.

$$GL_n(K) = \{ A \in M_n(K) \mid \exists\, B \in M_n(K),\ AB = I_n = BA \}$$

closed in $(M_n(K), \cdot)$

$(GL_n(K), \cdot)$ group (the general linear group of degree n)

ind. op

$K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ $\qquad A = (a_{ij})$

$A \in GL_n(K) \iff \underset{\sim\sim\sim}{\det A} \neq 0$ What det is? How do we compute it?

$$A^{-1} = \frac{1}{\det A} \cdot A^{*}$$

$$\underbrace{A^{*}}_{\text{the adjugate of } A} = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \dots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \dots & \alpha_{n2} \\ \vdots & \vdots & & \vdots \\ \alpha_{1n} & \alpha_{2n} & \dots & \alpha_{nn} \end{pmatrix}$$

$$\alpha_{ij} = (-1)^{i+j} \det A_{ij}$$

α_{ij}: compl. alg. al elem. a_{ij} " the cofactor of a_{ij}

$A_{ij} \in M_{n-1}(K)$: results from A by eliminating the i'th row and j'th column of A