Andererseits gilt für $n \geq 3$:

$A_n = \{\sigma \in S_n : \sigma$ lässt sich als Prod. von 3-Zykeln schreiben$\}$

In der Tat, A_n ist von Prod. $(ij)(kl)$ erzeugt $(i \neq j, k \neq l)$.

Aber $(ij)(jk) = (ijk)$ also $(ij)(kl) = (ij)(jk)(jk)(kl)$

$= (ijk)(jkl)$.

Jeder 3-Zykel ist aber ein Kommutator:

$(ijk) = (jk)(ij)(jk)(ij)$. Also $[S_n, S_n] = A_n, n \geq 3$.

(ii) $A_3 = \langle (123) \rangle$ abelsch $\rightsquigarrow$ Kommutatorreihe für S_3

$S_3 \rhd A_3 \rhd \{e\} \rightsquigarrow S_3$ auflösbar

(iii) Sei $n = 4$ und $V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \subset A_4$.

Wissen $V_4 \lhd S_4$ also $V_4 \lhd A_4$ (siehe Blatt 2 & 3) und

$\operatorname{ord}(A_4/V_4) = 3$ also $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ ist abelsch.

Insb. $[A_4, A_4] \subset V_4$ nach 1.7.2. Andererseits

$(12)(34) = (123)(124)(132)(142) = [(123),(124)]$ usw.

also $V_4 \subset [A_4, A_4]$.

Die Kommutatorreihe ist

$$S_4 \rhd A_4 \rhd V_4 \rhd \{e\}$$

$\rightsquigarrow S_4$ auflösbar.

(iv) Ist $n \geq 5$ so gilt $[A_n, A_n] = A_n$ denn z.B.

$(123) = (124)(135)(142)(153)$

Insbesondere ist S_n, $n \geq 5$, nicht auflösbar!

2. Ringe und Polynome

§2.1. Ringe

2.1.1. Def. Ein Ring ist eine Menge R mit zwei Verknüpfungen $+, \cdot$ (Addition, Multiplikation) so dass gilt:

(i) $(R,+)$ ist eine abelsche Gruppe (schreibe 0 für das neutr. Elem, $-a$ für das Inverse zu a)

(ii) Die Multiplikation ist assoziativ: $(ab)c = a(bc)$, $a,b,c \in R$.

(iii) Es gibt $1 \in R$ (Einselem) mit $a \cdot 1 = 1 \cdot a = a$, $a \in R$

(iv) Distributivgesetze: $a(b+c) = ab + ac$, $(b+c)a = ba + ca$

R heißt kommutativ falls $ab = ba$ für alle $a,b \in R$

Bem Manchmal verzichtet man auf (iii); dann heißt der Begriff aus 2.1.1. "unitärer Ring".

$(R,\cdot)$ ist i.A. keine Gruppe, denn die Existenz inverser Elem. wurde nicht vorausgesetzt (siehe z.B. $(\mathbb{Z},+,\cdot)$). Insb.

$ab = ac \not\Rightarrow b = c$.

Wir schreiben $a^0 = 1$, $a^{k+1} = a \cdot a^k$, $k \in \mathbb{N}_0$.

2.1.2 Lemma (Rechenregel) $\forall a,b \in R$ gilt:

$0 \cdot a = a \cdot 0 = 0$, $a(-b) = (-a)b = -ab$, $(-a)(-b) = ab$

Beweis $0 \cdot a + 0 \cdot a = (0+0)a = 0a \rightsquigarrow 0a = 0$

$a(-b) + ab = a(-b+b) = a \cdot 0 = 0 \rightsquigarrow a(-b) = -ab$

$(-a)(-b) = -(a(-b)) = -(-ab) = ab$.

2.1.3 Bem. Es gilt $R \neq \{0\} \Leftrightarrow 1 \neq 0$ ($R = \{0\}$ heißt Nullring)

„$\Leftarrow$" klar; „$\Rightarrow$" Wäre $1 = 0$, so $a = 1 \cdot a = 0 \cdot a = 0$ $\forall a \in R$.

2.1.4. Def (i) $S \subset R$ heißt Unterring von R, wenn $(S,+) < (R,+)$, $1 \in S$ und $a, b \in S \Rightarrow ab \in S$. Dann ist $(S,+,\cdot)$ Ring.

(ii) $R^* := \{a \in R : \exists b \in R \quad ab = ba = 1\}$ heißt die Menge der Einheiten von R. $(R^*, \cdot)$ ist Gruppe, genannt Einheitsgruppe von R.

(iii) Falls $R \neq \{0\}$, $R^* = R \setminus \{0\}$, so heißt R Schiefkörper. Ist $(R^*, \cdot)$ abelsch, so heißt R Körper.

(iv) $a \in R$ heißt Nullteiler, wenn $\exists b \in R \setminus \{0\} : ab = 0$ oder $ba = 0$

R heißt Integritätsring, wenn R kommutativ ist und kein $a \neq 0$ ist Nullteiler. Jeder Körper ist Int.ring.

2.1.5 Bsp. (i) $(\mathbb{Z}, +, \cdot)$ Integritätsring, $\mathbb{Z}^* = \{\pm 1\}$.

(ii) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ Ring, $(\mathbb{Z}/n\mathbb{Z})^* = \{\hat{a} : a \in \mathbb{Z}, ggT(a,n) = 1\}$

Insb. ist $\mathbb{Z}/p\mathbb{Z}$, p prim, ein Körper.

Ist $ggT(a,n) > 1$, so ist $\hat{a} \in \mathbb{Z}/n\mathbb{Z}$ Nullteiler.

(iii) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ Körper.

(iv) K Körper $\rightsquigarrow (M_{n\times n}(K), +, \cdot)$ Ring,

$M_{n\times n}(K)^* = \{A \in M_{n\times n}(K) : \det A \neq 0\} =: Gl_n(K)$

(v) X Menge, R Ring, $(Abb(X,R), +, \cdot)$ Ring, wobei für $f, g : X \to R$, $(f+g)(x) = f(x) g(x)$, $(fg)(x) = f(x) g(x)$.

2.1.6 Def. R, R' Ringe; $\varphi : R \to R'$ heißt Ringhomomorphismus wenn $\varphi(a+b) = \varphi(a)\varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in R$ und $\varphi(1) = 1$. $\ker\varphi := \{a \in R : \varphi(a) = 0\}$ heißt Kern von φ

φ heißt Ringisomorphismus, wenn φ bijektiver Ringhomom

2.1.7. Bem Sei $\varphi: R \to R'$ Ringhomom. Dann

(i) $\operatorname{Im}\varphi \subset R'$ Unterring (ii) $a \in R^* \Rightarrow \varphi(a) \in R'^*$
(Inverses ist $\varphi(a^{-1})$), also $\varphi|_{R^*}: R^* \to R'^*$ Gruppenhom.

(iii) R Körper, so ist φ injektiv
($a \neq 0 \Rightarrow a \in R^* \Rightarrow \varphi(a) \in R'^* \Rightarrow \varphi(a) \neq 0$)

Ab jetzt betrachten wir nur noch Kommutative Ringe.

§2.2 Polynomringe

2.2.1 Def Sei R Ring und $R^{(\mathbb{N}_0)} := \{f: \mathbb{N}_0 \to R : f(i) = 0 \text{ für fast alle } i \in \mathbb{N}_0\}$

Für $f = (a_i)_{i\in\mathbb{N}_0}$, $g = (b_i)_{i\in\mathbb{N}_0}$ setze

$f + g = (a_i + b_i)_{i\in\mathbb{N}_0}$, $f \cdot g = (c_i)_{i\in\mathbb{N}_0}$, $c_i = \sum_{\substack{\mu,\nu\in\mathbb{N}_0 \\ \mu+\nu=i}} a_\mu b_\nu$

Setze $X := (0,1,0,\dots)$. Dann $X^n = (0,0,\dots,\underbrace{1}_{\text{n-te Stelle}},0,\dots)$

$\rightsquigarrow f = (a_i)_{i\in\mathbb{N}_0} = a_0 + a_1 X + \dots + a_n X^n + \dots$

Also sind die obig definierte + und · die "üblichen" Addition und Multiplikation von Polynomen.

$R[X] := R^{(\mathbb{N}_0)}$ heißt Polynomring (in einer Var.) über R.

Bem. $R \to R[X]$, $a \mapsto (a,0,0,\dots)$ ist ein injektiver Ringhomom; wir identif. a zu $(a,0,0,\dots)$

Damit ist das Nullelem $0 = (0,0,\dots)$ und Einselem $1 = (1,0,0,\dots)$.

2.2.2 Def Sei $f = \sum a_i X^i$. Dann heißt a_i der i-te Koeffizient von f. Der Grad von f ist

$$\operatorname{grad} f := \begin{cases} \max\{i : a_i \neq 0\} & \text{falls } f \neq 0 \\ -\infty & \text{falls } f = 0. \end{cases}$$