Inhaltsangabe zur Vorlesung „Algebraische und Geometrische Strukturen in der Mathematik“

JProf.-Dr. Christoph Wockel

20. Juni 2014

Konstruktionen mit Zirkel und Lineal

1. Vorlesung (1. April)

- Wiederholung: die Konstruktion der komplexen Zahlen durch *Adjunktion* von einer formalen Variable i mit $i^2 = -1$.
- Notation: $\mathbb{C} = \mathbb{R}(i)$
- Lem.: $\mathbb{Q}(\sqrt{2}) := \{a + \sqrt{2} \mid a, b \in \mathbb{Q}\}$ ist ein Körper bzgl.

$$(a + \sqrt{2}b) + (c + \sqrt{2}d) = (a + c) + \sqrt{2}(b + d)$$
$$(a + \sqrt{2}b) \cdot (c + \sqrt{2}d) = (ac + 2bd) + \sqrt{2}(ad + bc)$$

Literatur: [SS09, §6.5]

2. Vorlesung (3. April)

- Veranschaulichung der Körperstruktur von $\mathbb{C}$ in der Zeichenebene.
- Def.: Die Menge der aus einer Teilmenge $M \subseteq \mathbb{C}$ konstruierbaren Punkte $\curlywedge M \subseteq \mathbb{C}$.
- Die 4 klassischen Probleme der Geometrie: Würfelverdopplung, Winkeldreiteilung, Quadratur des Kreises und Konstruktion regelmäßiger n-Ecke.
- Def.: Teilkörper und Körpererweiterung
- Satz: Für $M \subseteq \mathbb{C}$ mit $\{0,1\} \subseteq M$ ist $\curlywedge M$ ein Teilkörper von $\mathbb{C}$.
- Offensichtlich gilt auch $1 \in M \Rightarrow i \in \curlywedge M$ und $\{0,1\} \subseteq M \Rightarrow \mathbb{Q} \subseteq \curlywedge M$ (sogar $\{0,1\} \subseteq M \Rightarrow \mathbb{Q} + i\mathbb{Q} \subseteq \curlywedge M$). Insbesondere ist jedes $z \in \mathbb{C}$ durch Elemente aus $\curlywedge\{0,1\}$ approximierbar!

Literatur: [KM13, 20.1.3 und 22.1.1-3] und [LL07, 1.1-2]

3. Vorlesung (8. April)

- Satz: Für $\{0,1\} \subseteq M$ ist $\curlywedge M$ quadratisch abgeschlossen, es gilt also für $z \in \mathbb{C}$
$$z^2 \in \curlywedge M \Rightarrow z \in \curlywedge M.$$
- Satz: Für $\{0,1\} \subseteq M$ ist $\curlywedge M$ der *kleinste* quadratisch abgeschlossene Teilkörper von $\mathbb{C}$, der invariant unter komplexer Konjugation ist. Das heißt, das jeder Teilkörper $k \subseteq \mathbb{C}$, der $M \subseteq k$, k quadratisch abgeschlossen und
$$z \in k \Leftrightarrow \overline{z} \in k$$
erfüllt, schon $\curlywedge M$ enthält.
- Konzept des Erzeugens durch Eigenschaften, die stabil unter dem Bilden von Durchscnitten sind. $\rightsquigarrow \curlywedge M$ ist der von M erzeugte quadratisch abgeschlossene Teilkörper von $\mathbb{C}$.
- Def.: Der *Primkörper* eines Körpers E ist
$$\mathrm{Prim}(E) := \langle\{0,1\}\rangle = \bigcap \{k \leq E \mid k \text{ ist Teilkörper von } E\}.$$

Literatur: [KM13, 22.1.3 und 20.1.4]

4. Vorlesung (10. April)

- Def.: Sei $k \subseteq E$ Teilkörper und $M \subseteq E$ Teilmenge. Dann ist

$$k(S) := \bigcap \{F \subseteq E \mid F \text{ Teilkörper mit } k \subseteq F \text{ und } M \subseteq k\}$$

  der durch Adjunktion der Element von M zu k erzeugte Teilkörper.

- Bsp.: $\mathbb{C} = \mathbb{R}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ und für $\xi_3 := e^{\frac{2\pi i}{3}}$

$$\mathbb{Q}(\xi_3) = \{a + \xi_3 b \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

- Lem.: $k(M \cup N) = (k(M))(N) = (k(N))(M)$.

- Def.: Für $k \subseteq E$ Teilkörper heißt $[E : k] := \dim_k(E)$ der *Grad* von k über E (beachte: E ist in natürlicher Weise ein k-Vektorraum). $k \subseteq E$ heißt *endlich* falls $[E : k]$ endlich ist.

- Bsp.: $[\mathbb{C} : \mathbb{R}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(e) : \mathbb{Q}]$ und $[\mathbb{Q}(\pi) : \mathbb{Q}]$ nicht endlich.

- Gradsatz: $k \subseteq E$, $F \subseteq E$ Teilkörper mit $k \subseteq F$. Dann gilt
  - $k \subseteq E$ endlich $\Leftrightarrow$ $k \subseteq F$ und $F \subseteq E$ endlich
  - $[E : k] = [E : F] \cdot [F : k]$ falls $K \subseteq E$ endlich.
- Lem.: $[E : k] = 2 \Leftrightarrow$ es existiert $a \in E \setminus k$ mit $E = k(a)$ und $a^2 \in k$.
- Eine Körpererweiterung vom Grad 2 nennt man deshalb auch die Adjunktion der Quadratwurzel a.

Literatur: [KM13, 20.1.5 und Lemma 22.2 (Beweis)], [LL07, F.1.6]

5. Vorlesung (15. April)

- Def.: Sukzessive Adjunktion von Quadratwurzeln (SAQW).
- Satz: $z \in \mathbb{C}$ liegt genau dann in $\triangle M$ wenn $z \in L$ für einen Unterkörper $L \subseteq \mathbb{C}$ mit $L = \overline{L}$ und der aus $\mathbb{Q}(M \cup \overline{M})$ durch SAQW entstehet.
- Kor.: $x \in \mathbb{C}$ leigt genau dann in $\triangle M$, wenn es Unterkörper $k_0, ..., kN-$ von $\mathbb{C}$ gibt, so dass $k_0 = \mathbb{Q}(M \cup \overline{M})$, $[k_i : k_{i-1}] = 2$ für $i = 1, ..., n$ und $z \in k_n$ gelten. Insbesonder gilt dann

$$[\mathbf{k}(\mathbf{z}) : \mathbf{k}] \textbf{ ist eine Potenz von 2}.$$

- Erinnerung: das Minmalpolynom eines Vektorraumendomorphismus.
- Def.: $k \subseteq E$ Teilkörper, $a \in E$ algebraisch. Dann ist $m_{a,k}$ das Minimalpolynom des Endomorphismus

$$\mu_a \colon k(a) \to k(a), \quad x \mapsto a \cdot x$$

- Lem.: $m_{a,k}$ ist normiert, irreduzibel und hat a als Nullstelle. Es ist durch diese Eigenschaften eindeutig festgelegt.

Literatur: [KM13, 22.1.4-5 und 20.3.2]

6. Vorlesung (17. April) – Einschub zur Polynomdivision

- Bsp.: Für $i \in \mathbb{C}$ ist $m_{i,\mathbb{Q}}(X) = X^2 + 1$.
- Satz (Polynomdivision): Für einen Körper k und $p, q \in k[X]$ mit $\deg(q) \leq \deg(p)$ existieren eindeutige r, s mir

$$p = s \cdot q + r \quad \text{und} \quad \deg(r) < \deg(q).$$

- Def.: Teilbarkeit in Polynomringen

$$\text{ggT}(p, q) := \text{Element in } \{a \in k[X] : a \mid p, a \mid q, a \text{ normiert}\} \text{ mit maximalem Grad.}$$

- Satz: Erweiterter Euklidischer Algorithmus. Insbesondere existiert $\text{ggT}(p, q)$ immer und dieser ist eindeutig (da normiert).
- Satz: Die Primpolynome sind genau die irreduziblen Polynome.

Literatur: [KM13, 14.3.8, 5.3.3 und 16.1] (einen elementaren Beweis vom letzten Satz habe ich in der Literatur leider nicht gefunden)

7. Vorlesung (22. April) – Einschub zu Faktorringen

- Def.: Ring, Ideal, Ringhomomorphismus, Faktorring
- Lem.: Für ein Idela $I \subseteq R$ eines Ringes R ist R/I ein Ring, so dass die Quotientenabbildung $R \to R/I$ ein Ringhomomorphismus ist.
- Satz: Für einen Körper k und ein Polynome $p \in k[X]$ gilt

$$k[X]/p \cdot k[X] \text{ ist Körper } \Leftrightarrow p \text{ ist irreduzibel.}$$

Literatur: [KM13, 15.1, 15.5] (der Beweis vom letzten Satz geht analog zu dem er Aussage „$\mathbb{Z}/n \cdot \mathbb{Z}$ Körper $\Leftrightarrow$ n Primzahl“, wie zum Beispiel in den Übungen **P10** und **H8**.)

8. Vorlesung (24. April)

- Thm.: Sein $k \subseteq E$ ein Teilkörper und $a \in E$. Dann gilt:

  a) a ist algebraisch $\Leftrightarrow$ a ist Nullstelle eines Polynoms in $k[X]$.

  b) Ist a algebraisch und $m_{a,k}$ das Minimalpolynom von a über k mit $n = \deg(m_{a,k})$, dann gilt $[k(a) : k] = n$ und

  $$k(a) = \{\sum_{i=0}^{n-1} \lambda_i a^i \mid \lambda_0, ..., \lambda_{n-1} \in k\}$$

  als Teilmengen (bzw. Teilkörper) von E.

- Satz (Nullstellenkriterium): Sei $p \in k[X]$ mit $\deg(p) \in \{2, 3\}$. Dann ist p genau dann irreduzibel, wenn p keine Nullstelle in k hat.

- Theorem (Eisensteinkriterium): Sei $p \in \mathbb{Q}[X]$ mit ganzzahligen Koeffizienten $p(X) = \sum_{i=0}^{n} \lambda_i X^i$ mit $\lambda_i \in \mathbb{Z}$ für alle i. Falls eine Primzahl α existiert, so dass

$$\alpha \mid \lambda_i \text{ für } i < n, \alpha \nmid \lambda_n \text{ und } \alpha^2 \nmid \lambda_0$$

  gelten, dann ist p irreduzibel in $\mathbb{Q}[X]$.

- Satz (Reduktionskriterium): Sei $p \in \mathbb{Q}[X]$ mit ganzzahligen Koeffizienten $p(X) = \sum_{i=0}^{n} \lambda_i X^i$ mit $\lambda_i \in \mathbb{Z}$ für alle i. Falls eine Primzahl α existiert, so dass $\alpha \nmid \lambda$ gilt, dann gilt

$$\sum_{i=0}^{n} [\lambda_i] X^i \text{ irred. in } (\mathbb{Z}/\alpha \cdot \mathbb{Z})[X] \Rightarrow p \text{ irred. in } \mathbb{Q}[X].$$

- Bsp.: $X^3 - 2$ hat in $\mathbb{C}$ die Nullstellen $\sqrt[3]{2}$, $e^{\frac{4\pi i}{3}}\sqrt[3]{2}$ und $e^{\frac{2\pi i}{3}}\sqrt[3]{2}$, ist also irreduzibel in $\mathbb{Q}[X]$. Daraus folgt $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, also ist insbesondere $\sqrt[3]{2}$ nicht mir Zirkel und Lineal konstruierbar (das Delische Problem ist nicht lösbar).

Literatur: [KM13, 19.2] [LL07, 5.3]

9. Vorlesung (29. April)

- Wiederholung zu Polynomringen
- Kreisteilungspolynome

$$\Phi_\alpha(X) := X^{\alpha-1} + ... + X + 1$$

für α Primzahl und deren Irreduzibilität.

- Nicht-Konstruierbarkeit der regelmäßigen $\alpha = 7-, 11-, 13-, ...$ Ecke (falls $\alpha - 1$ keine Potenz von 2 ist)
- Satz: Für $\xi_n = e^{\frac{2\pi i}{n}}$ gilt

$$\xi_n \in \triangle\{0,1\} \Leftrightarrow [\mathbb{Q}(\xi_n) : \mathbb{Q}] \text{ ist Potenz von 2.}$$

- Thm.:

$$\xi_n \in \triangle\{0,1\} \Leftrightarrow n = 2^\ell p_1 ... p_r$$

mit $\ell \geq 0$ und $p_1, ..., p_r$ paarweise verschiedene Primzahlen der Gestalt $p_i = 1 + 2^{2^{k_i}}$.

- Satz: Für alle $\varphi \in [0,1[$, für die $e^{2\pi i\varphi}$ transzendent ist, ist die Dreiteilung des Winkels $e^{2\pi i\varphi}$ nicht möglich.

Literatur: [LL07, F 5.(10+11+13); 11.2]

10. Vorlesung (6. Mai)

- Quotientenkörper Quot(R) für einen Nullteiler-freien Ring R (also ein Ring, in dem $r \cdot s = 0 \Rightarrow r = 0$ oder $s = 0$ gilt).
- Satz: Ist R ein Nullteiler-freier Ring. Ist p irreduzibel in $R[X]$, dann ist p auch irreduzibel in $(\mathrm{Quot}(R))[X]$.
- Allgemeines Eisensteinkriterium
- Thm.: e und π sind transzendent.

Literatur: [KM13, 13.8] und dieses Dokument zur Transzendenz von e von Rudolf Fritsch.

11. Vorlesung (8. Mai)

- Def.: Monoid, Gruppe, Homomorphismus, Ordnung einer Gruppe
- Elementare Beispiele: $(\mathbb{Z}, +)$, $(k, +)$ und $(k \setminus \{0\}, \cdot)$ für k Körper, $\mathrm{Sym}(X)$ für X Menge, $\mathrm{GL}(V)$ für V Vektorraum, $\mathrm{GL}_n(k)$
- Beispiele für Homomorphismen: $(\mathbb{Q}, +) \to (\mathbb{R}, \cdot)$ $x \mapsto e^x$, $\mathrm{GL}_n(k) \cong \mathrm{GL}(V)$ falls $\dim(V)$ endlich
- Kurzschreibweisen: $g_1 \circ g_2 \circ ... \circ g_n$, multiplikative Schreibweise von Gruppen und additive Schreibweise von kommutativen Gruppen
- Lem.:
  1. $xg = h \Rightarrow x = hg^{-1}$ und $gx = h \Rightarrow x = g^{-1}h$
  2. $(gh)^{-1} = h^{-1}g^{-1}$ und $(g^{-1})^{-1} = g$
  3. $g^n g^m = g^{n+m} = g^m g^n$, $(g^m)^n = g^{n \cdot m} = (g^n)^m$ und $ab = ba$ impliziert $(ab)^n = a^n b^n$
- Bsp.: $\mathrm{SL}_n(k) \leq \mathrm{GL}_n(k)$, $\mathrm{SL}_2(\mathbb{Z}) \leq \mathrm{SL}_2(\mathbb{Q})$

- Def.: Erzeugte Untergruppe, Erzeugendensystem, zyklische Untergruppe, Ordnung eines Elements $\mathrm{ord}(g)$
- Satz: Sei G eine Gruppe und $g \in G$.

  1. Sei $\mathrm{ord}(g)$ endlich. Dann ex. ein minimales $n \in \mathbb{N}_{>0}$ mit $g^n = e$. Für dieses n gilt $\mathrm{ord}(g) = n$.

  2. Es gilt:

     $$\mathrm{ord}(g) \text{ nicht endlich } \Leftrightarrow g^n \neq g^m \text{ für alle } m \neq n$$

  3. Ist $\mathrm{ord}(g) = n$ endlich, so gilt $\mathrm{ord}(g^s) = \frac{n}{\mathrm{ggT}(n,s)}$

Literatur: [JS06, §I.1]

12. Vorlesung (13. Mai)

- Def.: Zyklische Gruppe
- Satz: Untergruppen zyklischer Gruppen sind zyklisch und korrespondieren zu Teilern der Ordnung.
- Nebenklassen G/H und Transversalen einer Untergruppe $H \leq G$
- Def.: Der Index $[G : H] := |G/H|$ einer Untergruppe $H \leq G$.
- Satz: Für $N \leq G$ und $M \leq N$ gilt

$$[G : M] = [G : N] \cdot [N : M]$$

- Kor.: G endlich und $H \leq G \Rightarrow |G| = |H| \cdot [G : H]$
- Kor.: G endlich, $g \in G \Rightarrow \mathrm{ord}(g)$ teilt $|G|$ und $g^{|G|} = e$
- Def.: Eulersche φ-Funktion

$$\varphi(n) := \{s \in \mathbb{N}_{>0} \mid s < n \text{ und } \overline{s} \text{ erzeugt } \mathbb{Z}_n\}$$

Literatur: [JS06, §I.1]

13. Vorlesung (15. Mai)

- Lem.: Im Folgenden sei G eine endliche Gruppe. Es gilt

  1. $\mathbb{Z}_n$ hat genau $\varphi(n)$ Elemente $[s]$ mit $0 < s \leq n$ und $\mathrm{ggT}(s,n) = 1$. Außerdem gilt $\sum_{d|n} \varphi(d) = n$.

  2. $\mathrm{ggT}(m,n) = 1 \Rightarrow m^{\varphi(n)} \equiv 1 \bmod n$

  3. p Primzahl, $m \in \mathbb{Z} \Rightarrow m^p \equiv m \bmod p$

  4. $|G| = p$ mit p Primzahl $\Rightarrow G$ ist isomorph zu $\mathbb{Z}_p$.

  5. $H \leq G$, $H' \leq G$ mit $\mathrm{ggT}(|H|, |H'|) = 1 \Rightarrow H \cap H' = \{e\}$.

- Def.: Normale Untergruppen (Notation: $H \trianglelefteq G$).

- Lem.: Für $H \leq G$ sind äquivalent

  1. $H \trianglelefteq G$

  2. $g^{-1}Hg = H$ für alle $g \in G$

  3. $gH = Hg$ für alle $g \in G$

- Lem.: Für $N \trianglelefteq G$: Faktorgruppe auf G/N und Homomorphismus $G \to G/H$.
- Bsp.: $\mathrm{SL}_n(k) \trianglelefteq \mathrm{GL}_n(k)$.
- Def.: Kern ($\ker(\varphi)$) und Bild ($\mathrm{im}(\varphi)$) eines Gruppenhomomorphismus.
- Satz: Für einen Gruppenhomomorphismus $\varphi\colon G \to H$ gilt
    1. $\varphi(g)^n = \varphi(g^n)$ für alle $n \in \mathbb{Z}$.
    2. $\ker(\varphi) \trianglelefteq G$ und $\mathrm{im}(\varphi) \leq H$.

Literatur: [JS06, Bemerkung nach Satz 1.13, §I.2, Beispiel vor Satz 4.4]

14. Vorlesung (20. Mai)

- Satz: Jede normale Untergruppe ist Kern eines Homomorphismus.
- Def.: Die Symmetrische Gruppe $S_n := \mathrm{Sym}(\{1, ..., n\})$. Wir nenne die Elemente von S_n auch Permutationen.
- Lem.: $|S_n| = n!$
- Def./Bem.: Träger einer Permutation, Zykelschreibweise, Transposition.
- Def./Bem.: Signum $\mathrm{sgn}(\pi)$ einer Permutation,

$$\mathrm{sgn}(\pi \circ \pi') = \mathrm{sgn}(\pi) \circ \mathrm{sgn}(\pi'),$$

und die alternierende Gruppe $A_n \trianglelefteq S_n$

- Satz:
  1. Jede Permutation kann als Produkt von Zykeln mit disjunktem Träger geschrieben werden. Die Faktoren in diesem Produkt sind bis auf Reihenfolge eindeutig bestimmt.
  2. Für $\pi \in S_n$ und den Zykel $(m_1 \ldots m_k)$ gilt
  $$\pi \circ (m_1 \ldots m_k) \circ \pi^{-1} = (\pi(m_1) \ldots \pi(m_k))$$
  3. S_n wird von den Transpositionen erzeugt.
  4. Ist p eine Primzahl, so wird S_p erzeugt von $\{\pi, \pi'\}$, wobei π ein Beliebiger Zyklus der Länge p ist und π' eine beliebige Transposition.
- Bem.:
  1. $|A_n| = \frac{n!}{2}$
  2. Ist $n \geq 3$, so wird A_n erzeugt von den Zykeln der Länge 3.

Literatur: [JS06, §I.3]

15. Vorlesung (22. Mai)

- Erinnerung: direkte Produkte von Gruppen.
- Def.: Gruppenwirkung (Notation $G \curvearrowright X$), G-Menge.
- Lem.: Eine Gruppenwirkung $G \curvearrowright X$ sind dasselbe wie ein Homomorphismus $G \to \mathrm{Sym}(X)$.
- Def./Bem.: Bahn $G.x$, Partition von X durch Bahnen, treue und transitive Wirkung.
- Def.: Homomorphismus von G-Mengen.
- Bsp.: $G \curvearrowright G$ durch Linkmultiplikation und durch Konjugation, $\mathrm{Sym}(X) \curvearrowright X$ durch $\pi.x := \pi(x)$, $G \curvearrowright G/H$ für $H \leq G$ durch $g.(xH) := (g \cdot h)H$.
- Def.: Fixpunkt, Isotropiegruppe/Stabilisator G_x, freie Wirkung
- Lem.: $G_x \leq G$ und $G_{(g.x)} = g \cdot g_x \cdot g^{-1}$

- Bsp.: Die Konjugationswirkung hat der Zentrum einer Gruppe als Fixpunkte und die Zentralisatioren als Stabilisatoren.
- Satz (Bahnformel): Ist $G \curvearrowright X$ eine Wirkung, dann ist für jedes $x \in X$ die Abbildung

$$p\colon G/G_x \to G.x, \quad gG_x \mapsto g.x$$

ein wohldefinierter Isomorphismus von G-Räumen.

Literatur: [JS06, §I.6]

16. Vorlesung (27. Mai)

- Satz (von Cauchy): Ist G endliche Gruppe, p Primzahl und $p \mid |G|$, so existiert in G ein Element der Ordnung p.
- Def.: Kommutatorgruppe G' und höhere Kommutatorgruppen $G^{(n)}$.
- Lem.: $G^{(n+1)} \trianglelefteq G^{(n)}$
- Lem.: Sei $N \trianglelefteq G$. Dann gilt

$$G/N \text{ abelsch} \Leftrightarrow G' \subseteq N.$$

- Bsp.: $G' = \{e\}$ falls G abelsch. $S_n' = A_n$ für alle $n \geq 1$, $A_n' = A_n$ für $n \geq 5$.
- Def.: G endlich heißt *auflösbar* falls $G^{(n)} = \{e\}$ für ein $n \in \mathbb{N}$ gilt.
- Bsp.: S_n ist auflösbar für $n \leq 4$ und nicht auflösbar für $n \geq 5$.
- Satz: Untergruppen und Faktorgruppen von auflösbaren Gruppen sind wieder auflösbar.

- Def.: Auflösbarkeit eines Polynoms $p \in \mathbb{Q}[X]$.
- Bsp.: Quadratische Polynome und $X^n - a$ ist für jedes $a \in \mathbb{Q}_{>0}$ auflösbar.

Literatur: [JS06, Satz 1.2] [Fis13, Abschnitt I.7.4 und III.5.10]

17. Vorlesung (03. Juni)

- Def.: Für $p \in \mathbb{C}[X]$ sei $\mathrm{NS}(p)$ die Menge der Nullstellen. Für $p \in k[X]$ für einen Unterkörper $k \subseteq \mathbb{C}$ ist $k(\mathrm{NS}(p))$ der *Zerfällungskörper* von p.
- Im Folgenden wird k immer ein Teilkörper von $\mathbb{C}$ sein!!!
- Bsp.: Für $p = X^n - a$ gilt $\mathbb{Q}(\mathrm{NS}(p)) = \mathbb{Q}(\xi_n, \sqrt[n]{a})$. Für $q = X^4 - 5X^2 + 6 = (X^2 - 2)(X^2 - 3)$ gilt $\mathbb{Q}(\mathrm{NS}(q)) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
- Def.: Für $p \in k[X]$ bezeichnet

$$\mathrm{Gal}_k(p) := \{\varphi \in \mathrm{Aut}(k(\mathrm{NS}(p))) \colon \ \varphi|_k = \mathrm{id}_k\}$$

  die *Galois-Gruppe* von p über k.
- Bsp.: Für $p = X^2 - 2$ ist $\mathrm{Gal}_{\mathbb{Q}}(p) = \{\mathrm{id}, \varphi\}$, wobei φ gerade $\sqrt{2}$ auf $-\sqrt{2}$ abbildet.
- Lem.: $\varphi \in \mathrm{Gal}(p), \alpha \in \mathrm{NS}(p) \Rightarrow \varphi(\alpha) \in \mathrm{NS}(p)$. Es wirkt also $\mathrm{Gal}(p)$ auf $\mathrm{NS}(p)$. Ferner ist $\varphi \in \mathrm{Gal}(p)$ *eindeutig* durch die Wirkung auf $\mathrm{NS}(p)$ bestimmt.

- Satz: $p \in \mathbb{C}[X]$ irreduzibel $\Rightarrow$ jede Nullstelle von p hat Vielfachheit 1.
- Satz: Sei $p \in k[X]$ und $p = g \cdot h$ mit g irreduzibel. Dann gilt

  1. $\alpha \in \mathrm{NS}(g)$ und $\varphi \in \mathrm{Gal}_k(p) \Rightarrow g(\varphi(\alpha)) = 0$
  2. $\alpha, \beta \in \mathrm{NS}(g) \Rightarrow \exists\ \varphi \in \mathrm{Gal}_k(p)$ mit $\varphi(\alpha) = \beta$.

  Es operiert also $\mathrm{Gal}_k(p)$ transitiv auf den Nullstellen der irreduziblen Faktoren von p.

Literatur: [Fis13, §III.5]

18. Vorlesung (05. Juni)

- Kor.: Hat $p \in k[X]$ nur einfache Nullstellen dann gilt

$$\mathrm{Gal}_k(p) \text{ wirkt transitiv auf } \mathrm{NS}(p) \Leftrightarrow p \text{ ist irreduzibel}$$

- Thm.: Für $p \in k[X]$ gilt $|\operatorname{Gal}_k(p)| = [k(\mathrm{NS}(p)) : k]$.
- Für $p = X^4 - 5X^2 + 6$ ist $\mathrm{Gal}_{\mathbb{Q}}(p) \cong \{\mathrm{id}, (12), (34), (12)(24)\}$.
- Für $p = X^4 - 1$ gilt $\mathrm{Gal}_{\mathbb{Q}}(p) = \{\mathrm{id}, \varphi\}$, wobei φ die Einschränkung der komplexen Konjugation ist.
- Für $p = X^4 - 2$ ist $\mathrm{Gal}_{\mathbb{Q}}(p)$ die Symmetriegruppe des Quadrats.
- Satz: Ist $p \in \mathbb{Q}[X]$ irreduzibel, hat Primzahlgrad und genau zwei nicht-reelle Nullstellen, so gilt $\mathrm{Gal}_{\mathbb{Q}}(p) \cong S_n$.
- Thm.: Ein Polynom $p \in \mathbb{Q}[X]$ ist genau dann auflösbar, wenn seine Galois-Gruppe auflösbar ist.
- Bsp.: Falls $\deg p \leq 4$ so ist p auflösbar, weil S_n für $n \leq 4$ auflösbar ist.

- Bsp.: $p = X^5 - 4X + 2$ hat genau drei reelle Nullstellen, also auch genau zwei nicht-reelle Nullstellen. Damit ist $\mathrm{Gal}_{\mathbb{Q}}(p) \cong S_n$ nicht auflösbar und somit p auch nicht.

Literatur: [Fis13, §III.5]

19. Vorlesung (17. Juni)

- Beispiele von Objekte, die wir als Flächen im $\mathbb{R}^3$ ansehen wollen (Oberfläche einer Kugel, eines Torus, einer „Brezel“, Paraboloid, Hyperboloid) und von Objekten, die wir nicht als Flächen ansehen wollen (Flächen mit Ecken, Kanten Singularitäten oder Selbstschnitten)
- Definition einer regulären Fläche
- Beispiel: affinie Ebenen, Funktionsgraphen (also z.B. ein Paraboloid)

- Eine Teilmenge $S \subseteq \mathbb{R}^3$ heißt *reguläre Fläche*, wenn für jedes $p \in S$ eine offene Umgebung $O_p \subseteq \mathbb{R}^3$, eine offene Teilmenge $U_p \subseteq \mathbb{R}^2$ und eine glatte Funktion $F_p \colon U_p \to \mathbb{R}^3$ existieren, so dass

  1. $F(U_p) = S \cap O_p$ und $F_p \colon U_p \to S \cap O_p$ ein Homömorphismus ist.
  2. Die Jacobimatrix $D_u F_p$ für alle $u \in U_p$ Rang 2 hat.

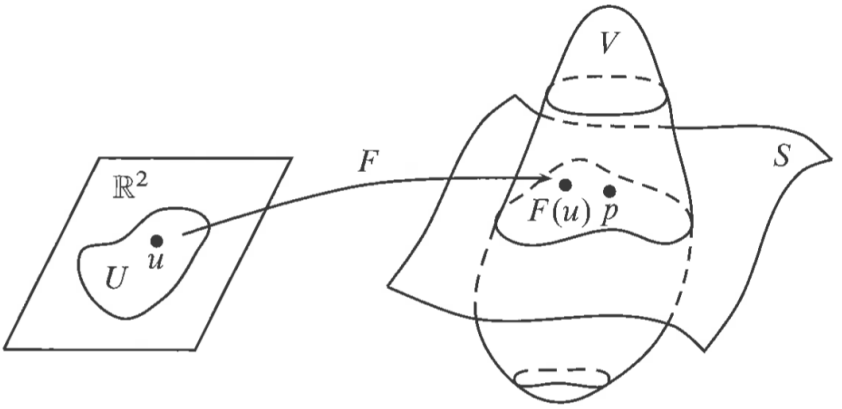

Abbildung 1: Eine lokale Parametrisierung

Literatur

[Fis13] Fischer, G. *Lehrbuch der Algebra* (Springer Spektrum, 2013). doi:10.1007/978-3-658-02221-1

[JS06] Jantzen, J. C. and Schwermer, J. *Algebra* (Springer Verlag, 2006). doi:10.1007/3-540-29287-X

[KM13] Karpfinger, C. and Meyberg, K. *Algebra (3. Auflage)* (Spektrum Akademischer Verlag, 2013). doi:10.1007/978-3-8274-3012-0

[LL07] Lorenz, F. and Lemmermeyer, F. *Algebra 1. Körper und Galoistheorie. (4. Auflage)* (Heidelberg: Elsevier/Spektrum Akademischer Verlag, 2007)

[SS09] Schichl, H. and Steinbauer, R. *Einführung in das mathematische Arbeiten* (Springer-Verlag, 2009). doi:10.1007/978-3-642-28646-9