Themen für das Lehramstspezifische Projekt und Referat zu „Algebraische und Geometrische Strukturen in der Mathematik“ SoSe 2014

Hinweise zur Bearbeitung:

- Einige der unten aufgeführten Aufgaben sind reine Literaturaufgaben. Das heißt, dass die Lösung zu der Aufgabe vollständig in den angegebenen Quellen zu finden ist. In diesem Fall besteht Ihre Aufgabe darin, den entsprechenden Sachverhalt so aufzuarbeiten und umzuformulieren, dass Sie zur Lösung der Aufgabe nur Wissen aus der Vorlesung verwenden.
- Bei den didaktischen Themen ist die Literaturrecherche und -rezeption wesentlicher Teil der Eigenleistung. Dementsprechend sind die Literaturverweise hier allgemeiner gehalten. Außerdem sollen Sie bei diesen Themen sich selbstständig weitere Literatur suchen, die hier angegeben Literatur soll Ihnen lediglich als Ansatzpunkt dienen.
- Für die fachmathematischen Themen ist Christoph Wockel (christoph@wockel.eu) Ihr Ansprechpartner, für die didaktischen Themen Armin Jentsch (armin.jentsch@uni-hamburg.de).

---

1 Lehramtsspezifische Projekte

~~**Thema 1.1** (Kubische Gleichungen, FM)~~
Sei k ein beliebiger Körper und $p = aX^3 + bX^2 + cX + d$ ein Polynom in $k[X]$ mit $\deg(p) = 3$. Stellen Sie die die Tschirnhaus-Transformation eines Polynom dritten Grades vor und erläutern Sie, warum es zur Lösung der Gleichung

$$p(X) = 0$$

ausreicht, eine explizite Lösungsformel für den Fall $a = 1$ und $b = 0$ zu kennen. Geben Sie dann die allgemeine Lösung der kubischen Gleichung

$$X^3 + pX + q = 0$$

in Abhängigkeit der Diskriminante $\Delta := -(4p^3 + 27q^2)$ an. Bestimmen Sie zum Schluss die Nullstellen und die Galois-Gruppe des Polynoms $7X^3 + 8X^2 + 8X + 1$.
Literatur: [Fis13, §5.2]

~~**Thema 1.2** (Endliche Körper I, FM)~~
Es sei k ein endlicher Körper.

1. Zeigen Sie, dass die Charakteristik $\mathrm{char}(k)$ immer endlich und immer eine Primzahl p ist.
2. Bestimmen Sie die Anzahl der reduziblen und irreduziblen Polynome vom Grad 2.
3. Zeigen Sie, dass es immer eine Körpererweiterung $k \subset k'$ gibt so dass k' genau $|k|^2$ viele Elemente hat.

4. Konstruieren Sie einen Körper, der 4 Elemente hat.

5. Konstruieren Sie einen Körper, der 81 Elemente hat.

6. Zeigen Sie, dass die unterliegende abelsche Gruppe von k immer isomorph zu $(\mathbb{Z}_p)^k$ ist falls $|k| = p^k$.

7. Es sei $\overline{k}$ ein Körper, der algebraisch abgeschlossen ist (also jedes Polynom in $\overline{k}[X]$ hat eine Nullstelle in $\overline{k}$) und der $k \subseteq \overline{k}$ als Teilkörper hat und der jede Nullstelle jedes Polynoms aus $k[X]$ enthält (ein abstrakter Satz besagt, dass ein solcher Körper immer existiert). Zeigen Sie, dass dann $[\overline{k} : k]$ nicht endlich sein kann.

8. Geben Sie einen Körper an, dessen Charakteristik endlich ist, der aber selber nicht endlich ist.

~~Thema 1.3~~ ~~(Klassifikation von Gruppen kleiner Ordnung, FM)~~

Klassifizieren Sie alle Gruppen der Ordnung kleiner gleich sieben. Genauer heisst das: geben Sie eine Liste von Gruppen der Ordnung kleiner gleich sieben an, so dass jede andere solchen Gruppe zu *genau einer* Gruppe aus dieser Liste isomorph ist. Eine ausführliche Begründung, warum jede Gruppe der Ordnung kleiner gleich sieben zu genau einer Gruppe aus der List isomorph ist, ist wesentlicher Teil der Aufgabe. Darüber hinaus sollten die Gruppen in der Liste solche Gruppen sein, die Sie aus der Vorlesung oder der Übung kennen.
Geben Sie außerdem mindestens 4 Gruppen der Ordnung 8 an, die paarweise nicht isomorph sind.

~~Thema 1.4~~ ~~(Konkrete Galois-Gruppen, FM)~~

Berechnen Sie jeweils die folgenden Galois-Gruppen:

1. $\mathrm{Gal}_{\mathbb{Q}}(p)$ mit $p(X) = X^4 + X^3 + X^2 + X + 1$
2. $\mathrm{Gal}_{\mathbb{Q}}(p)$ mit $p(X) = X^5 + X^4 + X^3 + X^2 + X + 1$
3. $\mathrm{Gal}_{\mathbb{Q}(i)}(p)$ mit $p(X) = X^4 - 2$

~~Thema 1.5~~ ~~(Potenzreihenringe, FM)~~

Es sei A ein kommutativer Ring. Es sei $A[[X]] := \{(f_0, f_1, f_2, ...) \colon f_i \in A\}$ die Menge aller Folgen in A. Wir können $f \in A[[X]]$ als Koeffizienten einer (nicht-abbrechenden) *Potenzreihe*

$$\sum_{n \in \mathbb{N}_0} f_n X^n$$

interpretieren. Zeigen Sie:

1. $A[[X]]$ wird bzgl.

$$(f+g)_n := f_n + g_n \quad \text{und} \quad (f \cdot g)_n := \sum_{i+j=n} f_i \cdot g_j$$

ein kommutativer Ring mit $0 = (0, 0, ...)$ und $1 = (1, 0, 0, ...)$.

2. Zeigen Sie: $A[[X]]$ ist genau dann nullteilerfrei wenn A dies ist (zur Erinnerung: ein Nullteiler in einem kommutativen Ring R ist ein Element $r \in R$, so dass es ein $s \in R \setminus \{0\}$ mit $r \cdot s = 0$ gibt).

3. Es ist $f \in A[[X]]$ genau dann multiplikativ invertierbar, wenn $f_0 \in A$ dies ist.

4. Bestimmen Sie in $\mathbb{Z}[[X]]$ das Inverse zu $1 - X$ und $1 - X^2$.

5. Zeigen Sie, dass
$$\mathfrak{m} := \{f \in A[[X]] \mid f_0 = 0\}$$
ein Ideal in $A[[X]]$ ist, ebenso wie $\mathfrak{m}^n$ für jedes $n \in \mathbb{N}_{>0}$.

6. Zeigen Sie, dass $\mathfrak{m}^n = X^n \cdot A[[X]]$ für alle $n \in \mathbb{N}_{>0}$ gilt.

7. Sei A ein Körper. Zeigen Sie, dass dann jedes Ideal in $A[[X]]$ von der Form $\mathfrak{m}^n$ für ein $n \in \mathbb{N}_{>0}$ ist.

   Hinweis: Betrachten Sie zu einem Ideal $\mathfrak{i}$ von $A[[X]]$ ein Element $f \in \mathfrak{i}$ so dass $\deg(f) := \min\{k \mid f_k \neq 0\}$ minimal unter allen Elementen in $\mathfrak{i}$ ist. Argumentieren Sie, dass dann $f \in \mathfrak{m}^n$ gilt. Aus der Darstellung $f = g \cdot X^n$ für ein $g \in A[[X]]$ können Sie dann mit Teil 3. schließen, dass $\mathfrak{i} = \mathfrak{m}^n$ gilt.

Beachten Sie, dass wir uns in dieser Aufgabe um Konvergenzfragen nicht zu kümmern brauchen. Allerdings kann man i.A. formale Potenzreihen nicht mehr als Funktionen von A nach A interpretieren.

~~Thema 1.6~~ ~~(Körpererweiterungen im Schulunterricht, D)~~

Entwickeln Sie eine Idee für eine Unterrichtseinheit zur Einführung der reellen Zahlen. Inwieweit würden Sie dabei auf die Kenntnisse der Vorlesung zurückgreifen?

Hinweis: Es soll geht hierbei nicht um eine konkrete Ablaufplanung mit Methoden, Sozialformen etc. gehen, sondern vor allem um Inhalte und Ziele.

~~Thema 1.7~~ ~~(Gruppentheorie im Schulunterricht, D)~~

Analysieren Sie, inwieweit sich das Thema „Gruppentheorie“ für den Schulunterricht eignet. Thematisieren Sie dabei insbesondere die hier bestehenden Verbindungen zum Rechnen modulo einer ganzen Zahl, welches ja in der Schule teilweise behandelt wird. Überlegen Sie sich, was geeignete Beispiele für Gruppen und Gruppenwirkungen sein könnten, die man im Schulunterricht gut motivieren könnte.

~~Thema 1.8~~ ~~(Konstruktionen mit Zirkel und Lineal im Schulunterricht, D)~~

Diskutieren Sie vor dem Hintergrund der Vorlesung, inwiefern dieses Thema zur Vernetzung von Algebra und Geometrie in der Schule besonders geeignet sein könnte. Gehen Sie u. a. auf das benötigte Vorwissen, Lernziele und Anwendungen ein. Welche Inhalte würden Sie genau behandeln?

~~Thema 1.9~~ ~~(Geschichte der Algebra)~~

Behandeln Sie die historische Entwicklung der allgemeinen Lösung von Gleichungen. Gehen Sie dabei insbesondere auf die Lösungsformel für quadratische Gleichungen (p-q-Formel) und die Galoistheorie ein.

Hinweis: Über [Bew13] hinaus soll in diesem Projekt der Teil der Literatur-Recherche besonders umfangreich sein.

2 Lehramtsspezifische Referate

~~**Thema 2.1** (Ein Ring mit nicht-eindeutiger Primfaktorzerlegung, FM)~~
Es sei $\mathbb{Z}[\sqrt{-5}] := \{a + bi\sqrt{5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

1. Zeigen Sie, dass $\mathbb{Z}[\sqrt{-5}]$ ist ein Unterring von $\mathbb{C}$ ist (also dass $(\mathbb{Z}[\sqrt{-5}], +)$ eine Untergruppe von $(\mathbb{C}, +)$ ist und $(\mathbb{Z}[\sqrt{-5}], \cdot)$ ein Untermonoid von $(\mathbb{C}, \cdot)$ ist).
2. Zeigen Sie, dass die Abbildung $z = (a, b) \mapsto \overline{z} = (a, -b)$ ein Automorphismus von $\mathbb{Z}[\sqrt{-5}]$ ist und dass die Normabbildung $|\cdot| \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0$, $(a, b) \mapsto a^2 + 5b^2 = z\overline{z}$ multiplikativ ist (also dass $|a \cdot b| = |a| \cdot |b|$ gilt).
3. Zeigen Sie, dass ± 1 die einzigen multiplikativ invertierbaren Elemente in $\mathbb{Z}[\sqrt{-5}]$ sind.
4. Es sei $x_1 = 3$, $x_2 = 2 + \sqrt{-5}$ und $x_3 = 2 - \sqrt{-5}$. Zeigen Sie, dass es für jedes Paar i, j mit $i \neq j$ kein multiplikativ invertierbares Element a gibt, für das $x_i = a \cdot x_j$ gilt.
5. Zeigen Sie, dass jedes x_i ein irreduzibles Element von $\mathbb{Z}[\sqrt{-5}]$ ist, dass also aus $x_i = a \cdot b$ folgt, dass a oder b multiplikativ invertierbar sein müssen.
6. Folgern Sie, dass sich 9 in $\mathbb{Z}[\sqrt{-5}]$ auf zwei verschiedene Weisen als Produkt von irreduziblen Elementen schreiben lässt, so dass sich die Faktoren nicht nur um ein multiplikativ invertierbares Element unterscheiden.
7. Zeigen Sie, dass das irreduzible Element 3 von $\mathbb{Z}[\sqrt{-5}]$ *kein* Primelement ist, dass es also $a, b \in \mathbb{Z}[\sqrt{-5}]$ gibt, so dass $3 \mid a \cdot b$ gilt, aber weder $3 \mid a$ noch $3 \mid b$.

~~**Thema 2.2** (Endliche Körper II, FM)~~
Es sei k ein beliebiger Körper.

1. Zeigen Sie, dass die Einheitengruppe $(k \setminus \{0\}, \cdot)$ von k zyklisch ist, falls k endlich ist.
2. Zeigen Sie: ist $p \in k[X]$ ein Polynom, so gibt es eine Körpererweiterung $k \subseteq E$, so dass E alle Nullstellen $\mathrm{NS}(p)$ enthält und $E = k(\mathrm{NS}(p))$ gilt.
3. Zeigen Sie: zu jeder Primzahlpotenz $q := p^n$ existiert bis auf Isomorphie genau ein Körper $\mathbb{F}_q$ mit q Elementen.

Literatur: [Fis13, Satz über den Zerfällungskörper in §III.2.3], [KM13, Korollar 14.9 und Satz 26.2]

Thema 2.3 (Algebraische Erweiterungen, FM)
Eine Körpererweiterung $k \subseteq E$ heißt *algebraisch*, falls jedes Element $a \in E$ algebraisch über k ist, also die Nullstelle eines Polynoms in $k[X]$ ist.

1. Es sei $k \subseteq E$ eine endliche Erweiterung, also $[E : k]$ endlich. Zeigen Sie, dass dann $k \subseteq E$ algebraisch ist.

   Hinweis: H6

2. Wir setzen $\mathrm{Alg}(E_k) := \{a \in E \mid a \text{ ist algebraisch über } k\}$. Zeigen Sie, dass $\mathrm{Alg}(E_k)$ ein Unterkörper von E ist und dass $k \subseteq \mathrm{Alg}(E_k)$ eine algebraische Erweiterung ist.

3. Berechnen Sie den Grad der Erweiterung $\mathbb{R} \subseteq \mathrm{Alg}(\mathbb{C}_{\mathbb{R}})$.

4. Zeigen Sie, dass $\mathrm{Alg}(\mathbb{C}_{\mathbb{Q}})$ eine algebraische Erweiterung von $\mathbb{Q}$ ist, die *nicht* endlich ist.

5. Zeigen Sie, dass $\mathrm{Alg}(\mathbb{C}_{\mathbb{Q}})$ algebraisch abgeschlossen ist, also dass jedes Polynom in $\mathrm{Alg}(\mathbb{C}_{\mathbb{Q}})$ eine Nullstelle in $\mathrm{Alg}(\mathbb{C}_{\mathbb{Q}})$ hat.

   Hinweis: Sie können per Widerspruchsbeweis zeigen, dass jedes Polynom in $\mathrm{Alg}(\mathbb{C}_{\mathbb{Q}})[X]$ schon eine Nullstelle haben muss.

Wir haben somit eine algebraische Körpererweiterung $\mathbb{Q} \subseteq \mathrm{Alg}(\mathbb{Q} \subseteq \mathbb{C})$ konstruiert, für die $\mathrm{Alg}(\mathbb{Q} \subseteq \mathbb{C})$ algebraisch abgeschlossen ist. Eine solche Erweiterung nennt man auch *algebraischen Abschluss* von $\mathbb{Q}$.

~~Thema 2.4 (Dieder-Gruppen und semi-direkte Produkte, FM)~~
Für $n \in \mathbb{N}_{>1}$ sei $\xi_n := e^{\frac{2pii}{n}}$ und

$$E_n = \{1, \xi_n, (\xi_n)^2, ..., (\xi_n)^{n-1}\}$$

die Eckpunkte eines regelmäßigen n-Ecks. Dann betrachten wir die von den beiden Elementen

$$\alpha \colon E_n \to E_n, \quad x \mapsto \overline{x} \quad \text{und} \quad \beta \colon E_n \to E_n, \quad x \mapsto \xi_n \cdot x$$

erzeugte Untergruppe D_n von $\mathrm{Sym}(E_n)$.

1. Visualisieren Sie die Wirkung von α und β auf dem regelmäßigen n-Eck E_n. Welchen geometrischen Operationen entsprechen die Permutationen α und β.

2. Zeigen Sie, dass $\mathrm{ord}(\alpha) = 2$, $\mathrm{ord}(\beta) = n$ und $\alpha \circ \beta \circ \alpha^{-1} = \beta^{-1}$ gilt.

3. Bestimmen Sie die Bahn und den Stabilisator $(D_n)_1$ von 1 bezüglich dieser Wirkung. Ist $(D_n)_1$ auch normal?

4. Geben Sie ein Element von $\mathrm{Sym}(E_n)$ an, welches nicht in D_n enthalten ist. Argumentieren Sie dabei genau, warum das Element nicht in D_n liegt.

5. Führen Sie das (äußere) semi-direkte Produkt $N \rtimes G$ von zwei Gruppen N und G ein, wenn zusätzlich noch ein Homomorphismus $G \to \mathrm{Aut}(N)$ gegeben ist. Geben Sie insbesondere eine explizite Formel für die Multiplikation und die inversen Elemente in $N \rtimes G$ an. Literatur hierzu ist z.B. [Fis13, §3.4]

6. Zeigen Sie, dass D_n isomorph zu $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ ist, wobei $\mathbb{Z}_2 \cong \{\pm 1\}$ auf $\mathbb{Z}_n$ durch Multiplikation wirkt.

7. Zeigen Sie, dass D_n für $n \geq 3$ nicht isomorph zu S_n ist.

8. Zeigen Sie, dass D_n nicht isomorph zu dem direkten Produkt $\mathbb{Z}_n \times \mathbb{Z}_2$ sein kann.

Thema 2.5 (Charakteristische Untergruppen, FM)
Eine Untergruppe $U \leq G$ heißt *charakteristisch* falls $\varphi(U) = U$ für alle $\varphi \in \mathrm{Aut}(G)$.

1. Zeigen Sie, dass Charakteristische Untergruppen immer normale Untergruppen sind.
2. Zeigen Sie, dass das Zentrum $Z(G)$ eine charakteristische Untergruppe von G ist.
3. Zeigen Sie, dass jede charakteristische Untergruppe einer normalen Untergruppe von G wieder eine normale Untergruppe von G ist.
4. Ist auch jede normale Untergruppe einer normalen Untergruppe von G normal in G?
5. Sei $H \leq G$ die einzige Untergruppe von G der Ordnung k. Zeigen Sie, dass H normal ist. Ist H auch charakteristisch?
6. Klassifizieren Sie für das direkte Produkt

   $$\mathbb{Z}_{p_1} \times ... \times \mathbb{Z}_{p_k}$$

   für paarweise verschiedene Primzahlen $p_1, ..., p_k$ alle charakteristischen Untergruppen.

~~**Thema 2.6** (RSA-Verschlüsselung)~~
Stellen Sie die Funktionsweise des RSA-Algorithmus dar und beantworten Sie die folgenden Fragen

1. Der Empfänger R der Nachricht wählt die Primzahlen $p = 11$ und $q = 13$. Wie lauten die möglichen öffentlichen Schlüssel von R?
2. R wählt den öffentlichen Schlüssel $(n, e) = (143, 7)$ und bekommt dem Sender S die Nachricht en $57, 42$ und 6 übermittelt. Wie lauten die entschlüsselten Nachrichten?

Diskutieren Sie, inwiefern sich die Funktionsweise des RSA-Algorithmus im Schulunterricht behandeln lässt. Gehen Sie dabei insbesondere auf das nötige Vorwissen der Schüler im Bereich des Rechnen in Restklassen ein.
Literatur: [KM13, Das RSA-Verfahren, S. 80]

~~**Thema 2.7** (Kryptographie im Schulunterricht, D)~~
Betrachten Sie andere Verschlüsselungsmethoden, wie das Diffie-Hellman Verfahren, das Pohlig-Hellman Verfahren, oder das ElGamal Verfahren im Hinblick auf die Verwendbarkeit im Schulunterricht. Gehen Sie dabei insbesondere auf das jeweils nötige Vorwissen in den entsprechenden Altersstufen ein. Thematisieren Sie außerdem, für welche Problematiken der modernen Kryptographie (Private-Key vs. Public-Key, Identifikation, Public-Key-Infrastrukturen,...) ein Schüler der entsprechenden Altersstufen sensibilisiert werden kann.
Literatur: [Buc08, KM13]

Thema 2.8 (Kubische Gleichungen im Schulunterricht, D)
Thematisieren Sie, inwiefern sich die allgemeine Lösungsformel der Nullstellen eines Polynoms dritten Grades im Schulunterricht thematisieren lässt. Gehen Sie dabei insbesondere auf das Fehlende Wissen über komplexe Zahlen und die Problematik des *casus irreducibilis* ein (den notwendigen Hintergrund

zur Lösungstheorie kubischer Gleichungen entnehmen Sie bitte [Fis13, §5.2] oder [Bew13, Kapitel 1+2]). Stellen Sie außerdem Bezüge zu dem Projekt „Komplexe Zahlen im Schulunterricht“ her.

~~**Thema 2.9** (Komplexe Zahlen im Schulunterricht, D)~~

Überlegen Sie sich, wie man die komplexen Zahlen in der Schule behandeln könnte: Diskutieren Sie mögliche Klassenstufen und liefern Sie Beispiele für Anwendungen. Beurteilen Sie außerdem, welche Darstellungen der komplexen Zahlen und welche ihre Eigenschaften besonders hilfreich sein können. Stellen Sie darüber hinaus Bezüge zu dem Projekt „Kubische Gleichungen im Schulunterricht“ her.

~~**Thema 2.10** (Geschichte der Algebra in der Schule, D)~~

Erläutern Sie in ihrem Vortrag, wie die Algebra in den Schulunterricht gelangt ist. Thematisieren Sie dazu z. B. die Meraner Reform und die „Neue Mathematik“.

Literatur

[Bew13] Bewersdorff, J. *Algebra für Einsteiger. Von der Gleichungsauflösung zur Galois-Theorie.* (Heidelberg: Springer Spektrum, 2013), 5th revised ed. edn. doi:10.1007/978-3-658-02262-4

[Buc08] Buchmann, J. *Introduction to cryptography. (Einführung in die Kryptographie.) 4th extended ed.* (Berlin: Springer. xxii, 274 p. EUR 29.95; SFR 49.00 , 2008)

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

[Hen12] Henn, H.-W. *Geometrie und Algebra im Wechselspiel. Mathematische Theorie für schulische Fragestellungen.* (Wiesbaden: Springer Spektrum, 2012)

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

[VW07] Vollrath, H.-J. and Weigand, H.-G. *Algebra in der Sekundarstufe* (Elsevier, Spektrum, Akad. Verl., 2007)