Seminar zur Algebra (Bachelor) — Sommersemester 2018

Prof. Dr. B. Richter

Dieses Seminar baut auf der Vorlesung Algebra I im Wintersemester 2017/18 auf. Falls Sie diese Vorlesung nicht besucht haben, müssten Sie den entsprechenden Stoff (Gruppen, Ringe, Körper bis einschliesslich Galoiskorrespondenz) eigenständig nachholen. Wir beschäftigen uns mit wichtigen Aspekten der Galoistheorie und einigen Anwendungen auf die Lösbarkeit von Gleichungen und auf Konstruierbarkeitsfragen: Wieso kann man zum Beispiel einen allgemeinen Winkel nicht mit Zirkel und Lineal dreiteilen? Wieso hat die *pq*-Formel Verallgemeinerungen für Polynome vom Grad 3 und 4, aber nicht ab Grad 5?

Falls Sie mit der angegebenen Literatur nicht zurecht kommen, schauen Sie bitte in die anderen angegeben Quellen; ggf. kann ich Ihnen alternative Literatur angeben.

Konzipieren Sie einen 80-minütigen Vortrag und eine 10-minütige Übungsphase, in der Sie den vorgetragenen Stoff mit den TeilnehmerInnen anhand von Beispielen vertiefen. Bitte geben Sie mir zwei Wochen vor Ihrem Vortrag eine Ausarbeitung ab.

Vorträge

(1) **Endliche Körper** Erklären Sie uns die Grundlagen über endliche Körper und zeigen Sie, dass jeder endliche Körper mit p^n Elementen ein Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$ ist. Definieren Sie den Frobenius-Automorphismus und bestimmen Sie die Galoisgruppe $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ [JS, §V.6]. Geben Sie explizite Modelle von $\mathbb{F}_{p^2}$ an [W, Aufgabe 2, 4, Seite 120].

(2) **Einheitswurzeln I** Definieren Sie, was n-te Einheitswurzeln sind für beliebige Körper und erklären Sie, was in endlicher Charakteristik passiert. Wann ist der Zerfällungskörper von $X^n - 1$ eine Galoiserweiterung? Definieren Sie das n-te Kreisteilungspolynom, zeigen Sie, dass es in $\mathbb{Z}[X]$ liegt und geben Sie explizite Beispiele an [JS, VI.2 bis einschließlich Satz 2.4].

(3) **Einheitswurzeln II** Zeigen Sie, dass die Kreisteilungspolynome irreduzibel sind über $\mathbb{Z}$ und erklären Sie, was über $\mathbb{F}_p$ passiert. Bestimmen Sie die Galoisgruppe des Zerfällungskörpers von $X^n - 1$, falls die Charakteristik des Körpers n nicht teilt. Beschreiben Sie Zwischenkörper von $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, falls p eine Primzahl ist [JS, VI.2 ab 2.5].

(4) **Hilberts Satz 90** Definieren Sie, was die Norm und die Spur einer endlichen Körpererweiterung sind und zeigen Sie grundlegende Eigenschaften dieser Abbildungen. Bringen Sie beides in Verbindung zum Minimalpolynom. Hilberts Satz 90 ist eine Aussage über Elemente mit Norm 1 bzw. Spur 0 in endlichen Galoiserweiterungen mit zyklischer Galoisgruppe [JS, VI.6].

(5) **Zyklische Erweiterungen** Betrachten Sie die Polynome $X^n - a$ und zeigen Sie, dass unter günstigen Umständen der Zerfällungskörper eine Galoiserweiterung mit zyklischer Galoisgruppe ist [JS, VI.4, bis Satz 4.2 mit Beweis]. Beschreiben Sie im Kontrast dazu zyklische Erweiterungen vom Grad p eines Körpers der Charakteristik p [L, Satz 3 mit Beweis in §14].

(6) **Auflösbarkeit von Gleichungen I** Erklären Sie, was es heisst, dass eine Körpererweiterung durch Radikale auflösbar ist und erläutern Sie, was dieser Begriff mit der Suche nach Nullstellen von Polynomen zu tun hat, die man in der Form iterierter, höherer Wurzeln aus den Koeffizienten schreiben kann. Zeigen Sie, dass diese Auflösbarkeit äquivalent ist zur Auflösbarkeit der entsprechenden Galoisgruppe [JS, Teile aus Abschnitt VI.5].

(7) **Auflösbarkeit von Gleichungen II** Machen Sie die Auslösbarkeit und Nichtauflösbarkeit von Gleichungen explizit, indem Sie zeigen, dass man alle polynomialen Gleichungen bis zum Grad 4 auflösen kann, dass es aber konkrete Gleichungen vom Grad fünf gibt, die nicht auflösbar sind. Geben Sie explizite Auflösungen für Gleichungen dritten Grades an. [JS, Teile aus VI.5], [L, Abschnitt §15.5 und Beispiel (ii) Seite 222].

(8) **Auflösbarkeit von Gleichungen III** Es gibt einen systematischen Weg, um Galoiserweiterungen mit Σ_n als Galoisgruppe zu konstruieren, und zwar über symmetrische Funktionen. Stellen Sie uns diese vor und natürlich auch die entsprechenden Galoiserweiterungen [L, §15.3].

(9) **Konstruierbarkeitsfragen und Körpererweiterungen** Was versteht man unter der Konstruierbarkeit mit Zirkel und Lineal? Beginnen Sie mit den Zahlen 0 und 1 in $\mathbb{C}$ und zeigen Sie, dass

die aus $\{0, 1\}$ konstruierbaren Zahlen einen Körper bilden. Zeigen Sie, dass dieser Körper unter Wurzelziehen abgeschlossen ist [L, bis Seite 8, ohne Beschreibung der "klassischen Probleme"].

(10) **Klassische Konstruktionsfragen und Adjunktion von Quadratwurzeln** Beschreiben Sie einige klassische Konstruktionsfragen (Dreiteilung des Winkels, Quadratur des Kreises etc) und erklären Sie den Zusammenhang zwischen konstruierbaren Zahlen und der sukzessiven Adjunktion von Quadratwurzeln [L, §1 Abschnitte 4 und 5 ohne Wiederholungen aus der Algebravorlesung].

(11) **Grade von Körpererweiterungen** Übersetzen Sie die bisherigen Ergebnisse in Aussagen über den Grad von Körpererweiterungen. Geben Sie damit Beweise für die Unlösbarkeit der klassischen Konstruierbarkeitsfragen an [L, §1 Abschnitt 6 ohne Wiederholungen aus der Algebravorlesung].

(12) **Legendre-Symbol** Es ist eine klassische Frage, wann eine Zahl n modulo einer Primzahl als Quadrat geschrieben werden kann. Antworten auf diese Frage sind wichtig, um zu entscheiden, ob Polynome in $\mathbb{F}_p[X]$ reduzibel sind. Das Legendre-Symbol sagt genau, ob dies möglich ist. Um dies auszurechnen, müssen wir verstehen, wie quadratische Erweiterungen in zyklotomischen Erweiterungen enthalten sind. [W, Abschnitte 15.4, 17.1], [L, Teile aus §11.3].

(13) **Quadratisches Reziprozitätsgesetz** Dieses Gesetz ist eine Symmetrieaussage für das Legendre-Symbol, welche Sie in diesem Vortrag beweisen [W, 17.2, 17.3], [L, Teile aus §11.3].

(14) $\bar{\mathbb{F}}_p$ **und unendliche Galoistheorie** Wie sieht der algebraische Abschluss von $\mathbb{F}_p$ aus? Beschreiben Sie ihn explizit [F, 3.3.6]. Geben Sie uns einen Ausblick auf unendliche Galoistheorie [N, IV, §1].

Literatur

[F] Gerd Fischer, Lehrbuch der Algebra, 4. Auflage, Springer, 2017.
[JS] Jens Carten Jantzen, Joachim Schwermer, Algebra, 2. Auflage, Springer, 2014.
[L] Falko Lorenz, Einführung in die Algebra, Teil I, 2. Auflage, B. I. Wissenschaftsverlag, 1992.
[N] Jürgen Neukirch, Algebraische Zahlentheorie, Springer, 1992.
[W] Gisbert Wüstholz, Algebra, Vieweg, 2004.