Prof. Dr. U. Görtz **SS 2018**

Bachelor-Seminar zur Algebra: Galois-Theorie

ECTS-Punkte: Das Seminar ist ein Bachelor-Seminar im Bachelorstudiengang Mathematik (oder Techno-/Wirtschaftsmathematik), das — für einen erfolgreichen Vortrag — 6 ECTS-Punkte erbringt. Der Vortrag kann nach Wahl des Sprechers auf Deutsch oder auf Englisch gehalten werden.

Erforderliche Vorkenntnisse: Gute Kenntnisse in Linearer Algebra 1 und 2, Analysis 1 und in Algebra 1 (Ringe, Ideale, Körpererweiterungen, endliche Körper, Galoistheorie).

Anschließende Bachelor-Arbeit: Die mit (*) markierten Vorträge eignen sich besonders gut, um daran eine Bachelor-Arbeit anzuschließen. Da dieses Seminar keine über die Vorlesung Algebra 1 hinausgehenden Voraussetzungen macht, wird das Thema der Bachelor-Arbeit eine Komponente enthalten, die den Vortragsinhalt etwas erweitert. Wenn Sie Interesse haben, Ihre Bachelor-Arbeit bei mir zu schreiben, sprechen Sie mich gerne frühzeitig an, damit ich Ihnen weitere Informationen geben kann.

Anforderungen an einen erfolgreichen Seminarvortrag.

- Ihr erstes und wichtigstes Ziel sollte sein, die im Vortrag zu behandelnde Mathematik gründlich zu verstehen. Das wird in der Regel eine ganz Menge Zeit in Anspruch nehmen; beginnen Sie daher frühzeitig mit Vorbereitung! Stellen Sie viele Fragen (sich und den anderen Seminarteilnehmern). Seien Sie diszipliniert darin, sich zu fragen, warum (ob) die im zugrundeliegenden Text aufgestellten Behauptungen richtig sind. Was lässt sich vereinfachen? Wenn Sie auf Dinge stoßen, die Sie nicht verstehen, fragen Sie die anderen Seminarteilnehmer (diejenigen, die die Vorträge direkt vor oder nach Ihnen halten, haben sich vielleicht schon genau dieselbe Frage gestellt). Vielleicht ist im Buch ein Fehler? Wenn Sie damit noch nicht weiterkommen, vereinbaren Sie einen Termin mit dem Assistenten, der das Seminar betreut.

- Wenn Sie die Mathematik verstanden haben, sollten Sie bewusst darüber nachdenken, wie Sie die Inhalte in Ihrem Vortrag darstellen möchten. Oft bietet es sich an, den Aufbau zu ändern, Sachen umzustrukturieren, zusätzliche Beispiele einzubauen, die Notation anzupassen, usw. — schließlich ist ein Vortrag etwas ganz anderes als ein geschriebener Text. Überlegen Sie im Vorfeld, was die Hauptpunkte Ihres Vortrags sind, die jeder Teilnehmer lernen sollte, und berücksichtigen Sie das entsprechend. Sie können nötigenfalls Sachen im Vortrag auslassen (zum Beispiel eine technische Rechnung, die zum Verständnis nicht notwendig ist (schauen Sie sie sich trotzdem genau an, um gegebenenfalls Fragen beantworten zu können!)). Denken Sie bei der Vortragsplanung darüber nach, was sich zum Weglassen eignet, damit Sie nicht am Ende wegen Zeitmangels gezwungen sind, die interessantesten Teile zu überspringen. Die Sachen, die Sie in der Vorbereitung besonders viel Zeit gekostet haben, sollten Sie nicht auslassen, denn die anderen Teilnehmer haben vermutlich ähnliche Schwierigkeiten beim Verständnis und können gerade an diesen Stellen viel lernen.

Anmerkungen zur Literatur. Wir richten uns meistenteils nach dem Buch [Hu] von Hungerford, einem der englischsprachigen Standardlehrbücher über Algebra. Alle Vortragsthemen werden aber auch mit kleinen Variationen in vielen anderen Algebrabüchern behandelt. Es lohnt sich sicher, auch einmal einen Blick in ein anderes Buch zu werfen, zum Beispiel in eines der Bücher von M. Artin (englisch), Bourbaki (englisch/französisch), Bosch (deutsch, [Bo]), Fischer (deutsch), Jantzen/Schwermer (deutsch), Lang (englisch), Lorenz (deutsch/englisch, [Lo]), Milne (englisch, `jmilne.org/math/`), ...

Vorträge

1. Der Hauptsatz der Galois-Theorie

Wir beginnen mit einer Erinnerung an den Hauptsatz der Galois-Theorie, für den wir im Seminar den Beweis von E. Artin kennenlernen wollen. Im Gegensatz zu dem Beweis aus der Vorlesung wird dabei vermieden, den Satz vom primitiven Element zu verwenden.

Vortragsinhalt: [Hu] V.2 (ohne Appendix). Teilweise sind die Ergebnisse aus der Vorlesung bekannt; diese Sachen sollten Sie dann entsprechend kurz abhandeln. Geben Sie jedenfalls die Aussage des Hauptsatzes der Galois-Theorie vollständig an, und erklären sie den Beweis.

2. Symmetrische Funktionen

Ein Ziel dieses Vortrags ist, für alle n eine Galois-Erweiterung L/K zu definieren (und zu verstehen), deren Galois-Gruppe isomorph ist zur symmetrischen Gruppe $\mathbf{S}_n$. (Daraus folgt — warum? — dass zu jeder endlichen Gruppe G eine Galois-Erweiterung existiert, deren Galois-Gruppe isomorph ist zu G.)

Vortragsinhalt: [Hu], V.2, Appendix.

3. Die Klassengleichung und Anwendungen

In diesem und dem folgenden Vortrag bauen wir unsere Kenntnisse der Gruppentheorie etwas weiter aus. Das wird uns später helfen, den Hauptsatz der Galoistheorie noch besser ausnutzen zu können.

Vortragsinhalt: [Hu] II.4 (Vieles davon ist eine Wiederholung von Ergebnissen, die aus der Vorlesung bekannt sind, und sollte entsprechend knapp behandelt werden. Neu ist die Klassengleichung in Cor. 4.4 (ii).). Dann [Hu] II.5 bis einschließlich Cor. 5.4. Beweisen Sie zusätzlich das Korollar, dass jede p-Gruppe auflösbar ist.

4. Die Sylow-Sätze

Nun beweisen wir die Sylow-Sätze, ein Standardergebnis über endliche Gruppen.

Vortragsinhalt: [Hu] II.5 von Lemma 5.5 bis zum Ende, und so viel von II.6, wie die Zeit noch erlaubt.

5. Der Fundamentalsatz der Algebra

In diesem Vortrag beweisen wir, mit Galois-Theorie und den Sylow-Sätzen, dass der Körper der komplexen Zahlen algebraisch abgeschlossen ist. Geben Sie auch den galois-theoretischen Beweis des Satzes vom primitiven Element (Lemma 3.17). Es sollte auch genügend Zeit sein, um die folgende Aussage zu beweisen:

Satz. Sei L/K eine endliche Körpererweiterung. Es existiert genau dann $\alpha \in L$ mit $L = K(\alpha)$, wenn die Erweiterung L/K nur endlich viele Zwischenkörper besitzt.

(Hier wird natürlich nicht vorausgesetzt, dass die Erweiterung L/K separabel ist. Geben Sie auch ein Beispiel einer Körpererweiterung an, die nicht die Eigenschaft des Satzes hat; je nachdem, wie viel Zeit Sie haben, brauchen Sie das nicht näher auszuführen.)

Vortragsinhalt: [Hu] V.3, Appendix. Für den hier formulierten Satz können Sie [Lo] Ch. 3, Thm. 5, zu Rate ziehen.

6. Die Galois-Gruppe eines Polynoms I

In diesem und dem folgenden Vortrag analysieren wir noch einmal genauer die Galois-Gruppe (des Zerfällungskörpers) eines Polynoms f, insbesondere in den Fällen, dass f Grad 3 oder 4 hat. Betrachtungen wie diese (und natürlich der unerfüllbare Wunsch, in ähnlicher Weise den Fall von Grad ≥ 5 zu verstehen) waren die wesentliche Motivation bei der Entwicklung der Galois-Theorie vor knapp 190 Jahren.

Vortragsinhalt: [Hu] V.4 bis einschließlich Lemma 4.10.

7. Die Galois-Gruppe eines Polynoms II

Vortragsinhalt: [Hu] V.4, von Prop. 4.11 bis zum Ende von V.4. Nach Möglichkeit auch Exercise 14.

8. Norm und Spur, Hilberts Satz 90

Dieser Vortrag ist etwas technischerer Natur. Er behandelt die wichtigen Begriffe der Norm und der Spur einer Körpererweiterung (die, wie wir sehen werden, eng mit den Begriffen der Determinante und der Spur von linearen Abbildungen zusammenhängen).

Vortragsinhalt: Definieren Sie Norm und Spur wie Lorenz, [Lo] Ch. 13, und beweisen Sie die dortige Feststellung F4 (mindestens im separablen Fall). Danach: [Hu] V.7 bis einschließlich Thm. 7.6.

9. Zyklische Erweiterungen

Mit den Hilfsmitteln aus dem vorangegangenen Vortrag können wir nun die Struktur zyklischer Erweiterungen noch besser als in der Vorlesung klären. Die aus der Vorlesung bereits bekannten Tatsachen sollten Sie wie üblich nur kurz wiederholen. Die Beweise der Sätze, die speziell Körper positiver Charakteristik betreffen, können Sie kurz halten, wenn es die Zeit erfordert.

Vortragsinhalt: [Hu] V.7, ab Prop. 7.7.

10. Kreisteilungskörper und auflösbare Erweiterungen (*)

Wir nehmen uns nun noch einmal die Kreisteilungskörper (oder zyklotomischen Körper) vor, d.h., die Erweiterungskörper, die durch Adjunktion von Einheitswurzeln entstehen. Danach bringen wir die Inhalte der vorherigen Vorträge zusammen, um zu beweisen, dass eine Körpererweiterung genau dann auflösbar ist, wenn sie durch Radikale auflösbar ist. (In der Vorlesung hatten wir nur den "wenn"-Teil gesehen, und eine Definition benutzt, die nur den Fall von Charakteristik 0 abdeckt.)

Für beide Abschnitte (z.B. Prop. 8.3, Thm. 9.4, viele Definitionen und einige weitere Sätze) gilt: Nutzen Sie das aus, was wir bereits in der Vorlesung bewiesen haben.

Vortragsinhalt: [Hu] V.8; außerdem von V.9 wenigstens die Ergebnisse.

11. Das quadratische Reziprozitätsgesetz (*)

In diesem Vortrag beweisen wir mit galoistheoretischen Methoden einen berühmten Satz der Zahlentheorie, das *quadratische Reziprozitätsgesetz*, das von Euler entdeckt und dann von Gauß um 1800 bewiesen wurde. Die Aussage zeigt eine verblüffende strukturelle Gesetzmäßigkeit der Menge der Primzahlen auf und ihre Verallgemeinerungen haben die Weiterentwicklung der algebraischen Zahlentheorie in den vergangenen 200 Jahren maßgeblich mitbestimmt, und tun es weiterhin.

Die wesentliche Aussage ist die folgende: Seien p und q verschiedene ungerade Primzahlen, und sei $p^* = (-1)^{\frac{p-1}{2}} p$. Dann sind äquivalent:

(i) Die Gleichung $x^2 \equiv q \mod p$ ist lösbar (mit $x \in \mathbb{Z}$).

(ii) Die Gleichung $x^2 \equiv p^* \mod q$ ist lösbar (mit $x \in \mathbb{Z}$).

(Das Auftreten des Vorzeichens $(-1)^{\frac{p-1}{2}}$ sollte Sie an die Übungsaufgaben 39 und 42 aus der Vorlesung erinnern.)

Vortragsinhalt: [Lo] 11.3 bis einschließlich Theorem 3.4; den Beweis von (34) können Sie gegebenenfalls auslassen. Außerdem ein Beispiel. Das dortige Theorem 3 haben wir bereits in den Übungsaufgaben zur Vorlesung bewiesen, daher können Sie es im Vortrag ohne Beweis verwenden.

12. Der erste Fall des großen Fermatschen Satzes für reguläre Primzahlen (*)

Dieser Vortrag ist schwieriger als die anderen.

Der *große Fermatsche Satz* (oder die *Fermatsche Vermutung*, auf Englisch: *Fermat's Last Theorem*) ist die folgende Aussage, die um 1640 als Randnotiz von P. de Fermat in eines seiner Bücher geschrieben wurde und deren Beweis 1995 von A. Wiles und R. Taylor nach Vorarbeiten vieler anderer Mathematiker vollendet wurde:

Theorem. Sei $n > 2$ eine natürliche Zahl. Dann hat die Gleichung

$$x^n + y^n = z^n$$

keine Lösung mit natürlichen Zahlen $x, y, z > 0$.

Wir wollen in diesem Vortrag den Satz unter den folgenden zusätzlichen Voraussetzungen beweisen ([Wa] Theorem 1.1), die im Vergleich zum allgemeinen Fall einen *wesentlich* einfacheren Beweis ermöglichen (der uns aber dennoch hinreichend fordern wird):

- Der Ring $\mathbb{Z}[\zeta_p]$ ist ein Hauptidealring (und damit insbesondere faktoriell). Äquivalent ist, dass die sogenannte Klassenzahl, die in der Aussage von [Wa] Thm. 1.1 auftritt, gleich 1 ist. Allerdings müssen Sie etwas Arbeit dabei investieren, herauszufinden, wo dies die Argumente von Washington vereinfacht (und dabei recherchieren, was die dort benutzten Begriffe jeweils bedeuten). Washington möchte diese Voraussetzung vermeiden, weil bekannt ist, dass sie nur für endlich viele Primzahlen richtig ist.
- Wir beweisen nur, dass es keine Lösungen x, y, z gibt derart, dass p keine der Zahlen x, y, z teilt.

Vortragsinhalt: [Wa] Theorem 1.1 mit der oben genannten Vereinfachung.

13. Topologische Gruppen

Zum Schluss untersuchen wir noch den Begriff der Galois-Erweiterung für unendliche algebraische Körpererweiterungen (zum Beispiel $\overline{\mathbb{Q}}/\mathbb{Q}$ und $\overline{\mathbb{F}}_p/\mathbb{F}_p$, wobei jeweils $\overline{K}$ einen algebraischen Abschluss von K bezeichne). Auch in diesem Fall ist es vernünftig, eine Erweiterung genau dann galoissch zu nennen, wenn sie normal und separabel ist. Allerdings bleibt der Hauptsatz der Galoistheorie *nur mit einer geeigneten Modifikation* gültig, die auf dem Begriff der topologischen Gruppe beruht. In diesem Vortrag treffen wir die notwendigen Voraussetzungen.

Definieren Sie die Begriffe des topologischen Raumes, der topologischen Gruppe, des projektiven Limes und der pro-endlichen Gruppe, und geben Sie jeweils Beispiele!

Vortragsinhalt: [Bo] 4.2, allerdings müssen Sie sich die relevanten Teile "zusammensuchen" und neu ordnen. Vergleiche auch [Ne] IV.1, IV.2. Weitere Hinweise und Referenzen für Beispiele gerne nach Absprache.

14. Unendliche Galois-Theorie

Formulieren und beweisen Sie den Hauptsatz der Galoistheorie für nicht notwendig endliche Galoiserweiterungen.

Vortragsinhalt: [Bo] 4.2, allerdings müssen Sie sich die relevanten Teile "zusammensuchen" und neu ordnen. Vergleiche auch [Ne] IV.1, IV.2. Weitere Hinweise und Referenzen für Beispiele gerne nach Absprache.

Literatur

[Bo] S. Bosch, *Algebra*, Springer 2006 (6. Auflage; oder eine andere Auflage)

[Hu] T. Hungerford, *Algebra*, Springer Graduate Texts in Math. **73**, 1974.

[Lo] F. Lorenz, *Algebra I: Fields and Galois Theory*, Springer 2006 (Von diesem Buch gibt es auch eine deutsche Fassung.)

[Ne] J. Neukirch, *Algebraic Number Theory*, Springer 1999 (Von diesem Buch gibt es auch eine deutsche Fassung.)

[Wa] L. Washington, *Introduction to Cyclotomic Fields*, Springer Graduate Texts in Math. **83**, 1982.

Anmerkungen. Zu Vortrag 10: Bei Hungerford wird auch nur der Fall von Charakteristik 0 behandelt. Es ist daher besser, sich an dem Buch von Bosch zu orientieren.