

Galoistheorie

Jürgen Behrndt

August 24, 2011

Abstract

1 VORWORT

Nun, es geht um die Theorie des Franzosen Evariste Galois 25.10.1811 - 31.5.1832 zur Bestimmung der Lösbarkeit von Polynomen beliebigen Grades. Ist nicht für ganz Dumme, aber das ist ja keiner hier, sondern dies Buch ist gedacht für Schüler ab der 10. Klasse oder Menschen vergleichbaren Wissens aller Altersklassen mit einem Basiswissen, was in etwa folgendes umfassen sollte:

- Bruchrechnung.
- Wissen was eine Wurzel ist oder schon mal davon gehört.
- Wissen was eine quadratische Gleichung ist und schon mal von der p/q Formel gehört.
- Mal was von Sinus, Kosinus und Logarithmus gehört.

Nützlich aber nicht unbedingt erforderlich sind Englischkenntnisse .

Benötigt werden hauptsächlich:

- Auffassungsvermögen.
- Interesse.
- Geduld.
- Spaß an Mathe.

Es werden Schritt für Schritt neue Begriffe mit vielen Beispielen und kleinen Aufgaben mit Lösungen eingeführt.

Am Ende wird der Hauptsatz der Galoistheorie stehen, die sog. Galoiskorrespondenz.

Gerade an seinem 200. Geburtstag am 25.10.2011 scheint mir eine Anerkennung des Werkes eines Mannes angebracht zu sein, der schon mit 20 in einem Duell starb, und seine Theorie als 18 jähriger fertiggestellt hatte, jedoch nicht verstanden wurde.

Man sagt er hätte die komplette Theorie in der Nacht vor seinem zu erwartendem Tod niedergeschrieben, jedoch richtig ist dass Galois es noch einmal hektisch überarbeitete und an verschiedenen Kollegen verschickte. unter anderem an C.F. Gauss, der aber keine Kenntnis davon nahm.

E.T Bell sagte über Galois:

”There is no completer example of the triumph of crass stupidity over untamable genius than is afforded by the brief life of Èvariste Galois.”

”Es gibt kein kompletteres Beispiel des Triumphes der krassen Dummheit über das unzählbare Genie, als das kurze Leben des Èvariste Galois.”

Ich finde jedoch, dass er seine geniale Arbeit getan hat, und der Rest kann verziehen werden.

Seit Dedekind die ersten Vorlesungen zum Thema (ca. 1850 in Braunschweig) hielt, wurde Galois endlich zur Kenntnis genommen.

(Literaturhinweise)

Er lebte zu Zeiten der französischen Revolution (Artikel aus Spektrum der Wissenschaft 1982) und auch zu Lebzeiten von Lagrange(1736 - 1813), Gauss(1777 - 1855), Poisson, Fourier(1768 - 1830), Niels Hendrik Abel, einem Norweger(1802 - 1829) u.a.

Zum Thema:

Der Leser wird behutsam geführt, und jeder Lernschritt soll sitzen, bevor es weitergeht.

Manches mag sich am Anfang schwierig anhören und die Galoistheorie ist normalerweise Stoff des 3. Semesters eines Mathematik-Hochschulstudiums.

Wenn man aber etwas wirklich verstanden hat, ist es einfach. Mathematik ist nicht schwer, wenn es hakt schauen wir genauer hin. Es gibt nichts ”Abstraktes”, wenn wir es wirklich SEHEN können. Nun können Sie die Augen zumachen und ein Fünfeck sehen, das linksrum rotiert?

Oder einen Würfel?

Das ist sehr anschaulich.

Und wenn man etwas geübt ist, kann man auch 4-dimensionale Räume und die Galoiskorrespondenz sehen!

Manchmal wird auch die Frage gestellt : Wobei ist die Galoistheorie überhaupt anwendbar?

Es gibt in der Quantenphysik sog. Divergenzen der Quantenfeldtheorie, die mit Hilfe von Galoissymmetrien erklärt werden können.

Und ein ganz ”einfaches ” Anwendungsobjekt ist der Rubiks Cube, aus den 80 ern noch bekannt.

Auch die engültige Lösung des Grossen Fermatschen Problems durch Andrew Wiles (1995) wäre ohne Galois undenkbar. (Literatur)

Wir wollen hier aber lieber etwas Zeit für die einfachen Grundlagen investieren, als Missverständnisse und Halbwissen zuzulassen, die später zu Unverständnis führen.

Nehmen sie keinen Satz als wahr hin, sagen Sie sich wirklich: stimmt das für mich? Und legen sich viele Zettel und Kugelschreiber hin!

1.1 Begriffe

Es werden folgende Begriffe eingeführt: (nicht erschrecken)

1. Mengen, Gruppen, unendliche und endliche.
2. Permutationen. Gerade und ungerade.
3. Abbildungen, transitive, surjektive, injektive, lineare.
4. Cyclenschreibweise einer Permutatition.
5. Modulo-Rechnung.
6. Die Symmetrische Gruppe S_n .
7. Ringe.
8. Polynome.
9. Polynomringe.
10. Körper.
11. komplexe Zahlen.
12. Einheitskreis.
13. Kreisteilungskörper.
14. Etwas Vektorrechnung.
15. Homomorphismen, Isomorphismen, Automorphismen, Automorphismengruppen.
16. Erweiterungskörper.
17. MinimalPolynome.
18. Irreduzibilität , Satz von Eisenstein.
19. hinreichende und notwendig Bedingungen. äquivalenz.
20. Zerfällungskörper.
21. Untergruppen.
22. (primitive) Einheitswurzeln.
23. Ordnung endlicher Untergruppen.
24. Normalteiler.
25. Radikale.
26. Auflösbarkeit von Gruppen und Polynomen.
27. Die Galoiskorrespondenz und der Hauptsatz.

28. Lösbarkeit von Polynomen in Radikalen.

Keine Angst, diese Begriffe brauchen hier und jetzt noch nicht verstanden zu werden.

Man mag manchmal fragen: Wozu brauche ich diesen Begriff, diesen Satz hier gerade?

Aber am Ende fügt sich alles zu einem großem Ganzen zusammen.

Galois entwickelte einen ganz neues Konstrukt, der das Lösungsproblem fast nebenbei erledigte, die sog. GRUPPE.

Jedes Teilgebiet, also Gruppen, Ringe, Körper, Automorphismen ist für sich in dutzenden Werken genauestens behandelt worden.

Ich will nicht zu tief in das sehr umfangreich gewordene interessanteste Gebiet der Gruppentheorie endlicher Gruppen eingehen, nur so weit als es zum Verständnis der Galoistheorie nötig ist.

Weiterführende Literaturhinweise finden sich am Ende.

Galois gilt als Mitbegründer oder an sich DER Gründer oder Erfinder oder Entdecker der Gruppentheorie. Wobei sich die Frage erheben mag ob es schon Gruppen gab, bevor man sie fand, was den Unterschied zwischen Entdeckung und Erfindung ausmacht.

Sicher gab es Pi bevor es Menschen gab, oder?

Das nur zum Grübeln.

Fokus und Ziel von E. Galois war jedoch die Lösung von quintischen Polynomen, also Gleichungen 5ten Grades etwa:

$$f(x) = x^5 + 2 \cdot x^4 - 3 \cdot x^3 + 5x^2 - 4x + 1$$

Man suchte seit langem eine Auflösungsformel für die Nullstellen Polynome höheren Grades.

Diese Fragestellung galt seit etwa dem 16. Jahrhundert als ungeklärt.

Für Gleichungen 3.ten und 4.ten Grades gab es schon Lösungsverfahren von Ruffini, Tartaglia, Scipione del Ferro (um 1530) und Cardano (1501-1576).

Übrigens derselbe Cardano, der die Kardanwelle erfand!

Die Italiener waren fleissig.

Es folgten noch Alexandre-Théophile Vandermonde (geb. 28. Februar 1735 in Paris; gest. 1. Januar 1796 in Paris), ein französischer Musiker, Mathematiker und Chemiker und besonders Joseph-Louis de Lagrange (geb 25. Januar 1736 in Turin als Giuseppe Lodovico Lagrangia, gest. 10. April 1813 in Paris.

Lagrange arbeitete hauptsächlich in Berlin.

Besonders Legendre's Buch *Éléments de géométrie* (1794) faszinierte Galois als 14 jährigen.

Und entfesselte seine Liebe zur Mathematik.

Sind also, so fragte er sich, solche Polynome wie $f(x)$ noch in verschachtelten Wurzelausdrücken, also durch eine Art p/q Formel lösbar?

Wenn nicht, vielleicht doch einige davon ?
Wieviele Lösungen gibt es dann, und wie sehen sie aus?
Um es vorwegzunehmen es gibt sie und sie sehen lustig aus.

Die Lösungen von

$$f_x = x^8 - 8 * x^7 + 24 * x^6 - 32 * x^5 + 18 * x^4 - 8 * x^3 + 8 * x^2 - 1 \text{ sind:}$$

$$x_i = 1 \pm \sqrt{(1 \pm \sqrt{-1 \pm \sqrt{2}})}$$

2

2.1 Mengen

2.1.1 eine injektive Abbildung

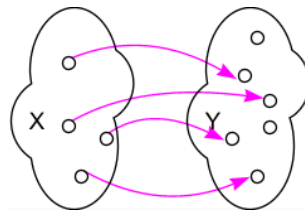


Figure 1: 2 Mengen und eine injektive Abbildung

3 Inhaltsverzeichnis, Seite 1 vorläufig.

3.1 Kapitel 1.

3.1.1 Mengen, Abbildungen, Bijektionen

3.1.2 Die p/q Formel.

3.1.3 Die "Mitternachtsformel".

3.1.4 Satz von Vieta.

3.1.5 Newton.

3.2 Kapitel 2.

3.2.1 Gleichungen 3. Grades

3.2.2 Cardano.

3.2.3 $x^3 - 2 = 0$

3.3 Kapitel 3.

3.3.1 Gruppen.

3.3.2 Beispiele.

3.3.3 \mathbb{N}

3.3.4 \mathbb{Z}

3.4 Kapitel 4.

3.4.1 Körper.

3.4.2 Beispiele: \mathbb{Q} \mathbb{Z}_p

3.5 Kapitel 5.

3.5.1 Ringe.

3.5.2 Ideale.

3.5.3 Restklassen.

3.5.4 $n\mathbb{Z}$.

3.5.5 Polynomringe.

3.5.6 $\mathbb{P}[x]$

3.5.7 Polynomdivision mit und ohne Rest.

3.5.8 Irreduzible Polynome.

3.5.9 Nebenklassen, Äquivalenzklassen, nullteilerfreie Ringe, primitive Restklassenkörper.

3.5.10 Beispiele.

4 Inhaltsverzeichnis, Seite 2 vorläufig.

4.1 Kapitel 5a.

4.1.1 Körpererweiterungen.

4.1.2 $Q(\sqrt{2})$

4.1.3 Abgeschlossenheit?

4.1.4 einfache Körpererweiterung.

4.1.5 algebraische Körpererweiterung.

4.1.6 normale Körpererweiterung.

4.1.7 separable Körpererweiterung.

4.1.8 galoische Körpererweiterung.

4.1.9 Beispiel für eine nicht normale Körpererweiterung.

4.2 Kapitel 5b.

4.2.1 Was man mit einem Viereck alles machen kann.

4.2.2 Permutationen.

4.2.3 Involutionen.

4.2.4 Transpositionen.

4.2.5 Zeichnungen und Diagramme.

4.3 Kapitel 5c.

4.3.1 Die Symmetrische Gruppe S_4 .

4.3.2 Zyklische Gruppen.

4.3.3 Ordnung eines Elementes, Satz von Lagrange.

4.3.4 konjugierte Elemente.

4.3.5 Kleinsche Vierergruppe

4.3.6 Diedergruppe.

4.4 Kapitel 6.

4.4.1 Algebraische Zahlen.

4.4.2 Minimalpolynom einer algebraischen Zahl.

4.4.3 Beispiele.

4.5 Kapitel 7.

4.5.1 Zerfällungskörper eines Polynoms.

4.5.2 Beispiel.

4.6 Kapitel 7a

4.6.1 Elementarsymmetrische Polynome.

4.7 Kapitel 8.

4.7.1 Radikale.

4.7.2 Komplexe Zahlen, eine Einführung.

4.7.3 Was heisst hier Wurzel?

5 Inhaltsverzeichnis, Seite 3 vorläufig.

5.1 Kapitel 9.

5.1.1 Einheitskreis

5.1.2 Einheitswurzeln.

5.1.3 Diagramme.

5.2 Kapitel 10.

5.2.1 Kreisteilungskörper.

5.3 Kapitel 11.

5.3.1 Untergruppen und Normalteiler.

5.3.2 Die Galoisgruppe eines Polynoms.

5.3.3 Beispiel aus S_4 .

5.4 Kapitel 12.

5.4.1 Normalreihen.

5.4.2 Subnormalreihen.

5.4.3 Kompositionsreihen.

5.4.4 Beispiel aus S_4 . und S_5

5.5 Kapitel 13.

5.5.1 Faktorgruppen.

5.6 Kapitel 14.

5.6.1 auflösbare Gruppen.

5.6.2 nicht auflösbare Gruppen.

5.6.3 einfache Gruppen.

5.7 Kapitel 15.

5.7.1 auflösbare Polynome.

5.7.2 nicht auflösbare Polynome.

5.7.3 einige Beispiele.

5.8 Kapitel 16.

5.8.1 Der Hauptsatz der Galoistheorie.

5.9 Kapitel 17

5.9.1 Einige Folgerungen.

5.10 Kapitel 18

5.10.1 Abschluss und Ausblicke

6 Nachwort

Angedachter Auszug aus letztem Kapitel (evtl):

Automorphismengruppen:

$$\text{Aut}(x^4 - 4 \mid \mathbb{Q})$$

$$\text{Aut}(x^4 - 2 \mid \mathbb{Q})$$

Zunächst faktorisieren wir die Polynome über \mathbb{C}

$$f = x^4 - 4 \stackrel{\mathbb{Q}}{=} \underbrace{(x^2 - 2)}_{f_1} \underbrace{(x^2 + 2)}_{f_2} \stackrel{\mathbb{R}, \mathbb{C}}{=} (x + \sqrt{2})(x - \sqrt{2})(x + i\sqrt{2})(x - i\sqrt{2})$$

$$g = x^4 - 2 \stackrel{\mathbb{R}, \mathbb{C}}{=} (x + \sqrt[4]{2})(x - \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2}) \text{ Feststellungen:}$$

f ist reduzibel Über \mathbb{Q}

g ist irreduzibel Über \mathbb{Q}

Welchen Einfluss hat das nun?

Kann ich im ersten Falle die Körpererweiterung in Etappen machen und sagen - dabei sei L der Zerfällungskörper von f_1 . Es sich ergibt sich insgesamt eine Körpererweiterung vom Grad 4 mit Minimalpolynomen $m_1 = x^2 - 2$ und $m_2 = x^2 + 1$ und

$$\text{Aut}(f \mid \mathbb{Q}) = \text{Aut}(f_2 \mid L) \times \text{Aut}(f_1 \mid \mathbb{Q}) \cong C_2 \times C_2 \cong V_4$$

Dabei ergibt sich der Isomorphietyp aus der transitiven Operation auf jeweils einer 2-elementigen Nullstellenmenge.

Alternativ müsste man zu einer beliebigen Permutation der Nullstellen prüfen, ob der dazugehörige Automorphismus auf dem Grundkörper die Identität ist.

Im zweiten Fall ist G schon irreduzibel über \mathbb{Q} . $\text{Aut}(g \mid \mathbb{Q})$ wirkt transitiv auf den 4 Nullstellen. Man weiß erst mal nur, dass es eine transitive Untergruppe der S_4 ist.

Den Grad der Körpererweiterung kann man hier nun aber auch bestimmen. Mit $m_1 = x^2 - 2$ und $m_2 = x^2 + 1$ ergibt sich eine Erweiterung vom Grad 8. Es ist $4! = 2^3 \cdot 3$ und daher ist die gesuchte Gruppe eine 2-Sylowgruppe in der S_4 . Daher gibt es nur einen möglichen Isomorphietyp (p-Sylowgruppen sind konjugiert). Nun weiß man entweder, dass es die D_8 ist oder...

Wie kann G nun auf den Nullstellen operieren? 2 sind komplex konjugiert (Grundkörper bleibt fix unter komplexer Konjugation). Bei entsprechender Nummerierung also (24) in G . Testet man nun, ob z.B. auch (1234) drin ist? Man bekommt keinen Widerspruch zu \mathbb{Q} muss fix bleiben. Daher auch (1234) in G . Damit haben wir eine (zyklische) Untergruppe der Ordnung 4. Somit ist sie vom Index 2 in G , also Normalteiler. Der Schnitt mit der Untergruppe (24) ist trivial. Die muss nun aber noch nicht Normalteiler sein. Wie operiert (24) auf (1234) bzgl. Konjugation? Dazu muss man sich nur

$$(24)(1234)(24) = (1432) = (1234)^{-1}$$

anschauen. Damit bekommt man ein Semidirektes Produkt und das ist dann die D_8 .

Literaturhinweise:

Condensed chapter from Men of Mathematics by E. T. Bell (1937), published by Simon and Schuster Pub. Co. DTH. This book is in the Math Lounge.

Adrien-Marie Legendre (18. September 1752 in Paris; - 10. Januar 1833 ebenda)

Andrew Wiles: Modular Elliptic Curves and Fermats last theorem. Annals of Mathematics 142 (1995), S.443 - 551.

Dieter Held: Die Klassifikation der endlichen einfachen Gruppen.