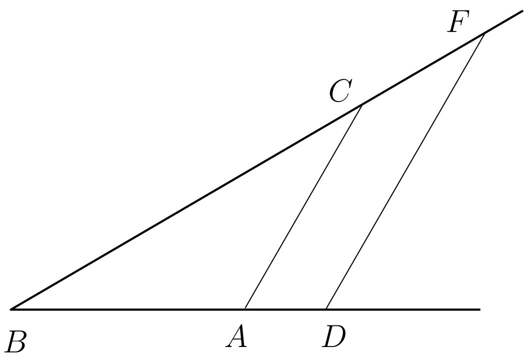
Geschichte der Mathematik, SS 2016
Kapitel VI und VII

Folie 117: Kapitel VI: Algebra im 17. und 18. JH

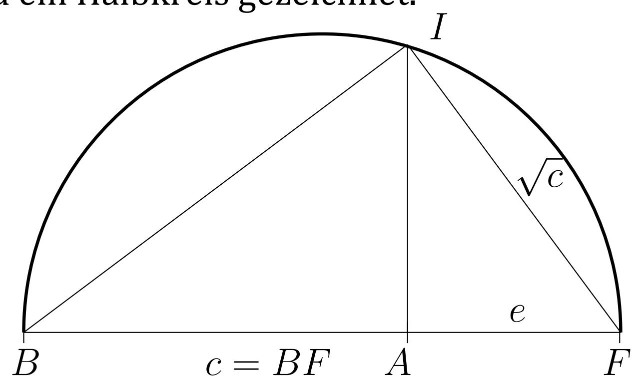
Auf die herausragenden Erfolge der Algebra im 16. JH folgte eine relative ruhige Periode. Die Aufmerksamkeit der Mathematik im 17. JH lag vor allem in der infinitesimalen Analysis, die zu der Zeit begründet wurde. Nichtsdestotrotz haben im Bereich der Algebra grundlegende Veränderungen stattgefunden, die man mit dem Wort Arithmetisierung charakterisieren kann.

Folie 118: Grössen als Strecken

Die ersten Schritte in diese Richtung wurden durch den Philosophen und Mathematiker René Descartes unternommen. Sein Werk *La Géométrie* (der 4. Teil vom *Discours de la méthode pour bien conduire sa raison et chercher la vérité dans les sciences* aus dem Jahr 1637) hat die Geometrie auf die Algebra reduziert, d.h. es hat die analytische Geometrie begründet. Darin hat Descartes zuerst Viètes Rechnungen mit Grössen transformiert: Descartes stellt alle Grössen durch Strecken dar und konstruiert eine Berechnungsmethode von Strecken, die sich grundlegend von derjenigen der Antike (die Basis für Viètes Konstruktion) unterschied. Seine Idee war, dass die Operationen mit Strecken (Längen) eine getreue Nachbildung der Operationen mit rationalen Zahlen sein solle. Während in der Antike und bei Viète das Produkt von zwei Strecken eine Fläche war (d.h. eine Grösse der Dimension 2), forderte Descartes, dass das Produkt auch ein Strecke sein solle. Um dies zu erreichen, führte er ein Einheitsstreck e ein und definierte das Produkt der Strecke a und b als die Strecke c, das das vierte Verhältnis der Strecke e, a und b sei.
Er hat einen beliebigen Winkel ABC genommen und hat die Strecken $AB = e, BD = b$ und $BC = a$. Dann hat er A und C verbunden und $DF \parallel AC$ gezeichnet. Damit hat er die Strecke $BF = c = ab$ erhalten (Strahlensätze, etwa $a: c = e: b$). Damit gehört das Produkt zur selben Grössenart (Strecken oder Längen) wie die Faktoren.



Division hat Descartes analog definiert. Will man $BF = c$ durch $BD = b$ dividieren, legt man von B aus die Strecke $BA = e$, sowie die Strecken $BF = c$ und $BD = b$ und verbindet D mit F. Parallel zu DF zeichnet man dann AC, die Strecke BC ist dann der gesuchte Quotient. Damit hat Descartes den Bereich der Strecken zu einer Nachbildung des Halbkörpers $\mathbb{R}^+$gemacht. Später hat er auch negative Strecken eingeführt (deren Richtung entgegengesetzt zu denjenigen der positiven Strecken waren), hat jedoch die Operationen mit negativen Zahlen nicht im Detail angeschaut. Schliesslich zeigte Descartes, dass man durch Wurzelziehen (Quadratwurzeln) von positiven Grössen nicht aus dem Bereich der Strecken rausfällt. (Ähnliche Überlegungen hat offenbar bereits Bombelli gemacht in Teilen seiner Algebra). Um die Quadratwurzel von $c = BF$ zu ziehen, hat Descartes auf dieser Strecke $e = AB$ abgetragen (falls $c > e$ ist). Über FB wird ein Halbkreis gezeichnet.



Und dann auf A eine Senkrechte gezogen, I sei der Schnittpunkt von dieser Senkrechten mit dem Halbkreis. Nach dem Kathetensatz ist dann die Strecke IF gerade $\sqrt{c}$ (denn ihr Quadrat ist $ec = c$). (Falls $c < e$ ist, trägt man FA auf die Verlängerung von BF nach links hin ab.)

Folie 119: Konventionen (Descartes)

Descartes führte die Konvention ein, Unbekannte mit den letzten Buchstaben des Alphabets zu bezeichnen, x, y, z, und bekannte mit den

Anfangsbuchstaben a, b, c. Sein Gleichheitszeichen war verschieden von dem heutzutage benutzten, es war ein auf dem Kopf stehendes æ (für aequalis, gleich), das mit der Zeit in etwa $\propto$ geschrieben wurde. Descartes hat sozusagen einen Isomorphismus zwischen dem Bereich der Strecken und dem Halbkörper $\mathbb{R}^+$der reellen (positiven) Zahlen gegeben. Er hat jedoch keine allgemeine Definition von Zahlen gegeben.

Folie 120: Newtons Definition von Zahlen

Eine allgemeine Definition von Zahlen hat Newton in seiner *arithmetica universalis* getan. Er schrieb: „Berechnungen werden entweder durch Zahlen gemacht, wie in der gewöhnlichen Arithmetik, oder durch allgemeine Variablen, so wie das analytische Mathematiker pflegen". Newton gibt eine allgemeine Definition von Zahlen – in der Antike war eine Zahl eine Sammlung von Einheiten (die natürlichen Zahlen), Verhältnisse von ähnlichen Quantitäten (reelle Zahlen) wurden nicht als Zahlen aufgefasst. Claudius Ptolemäus und arabische Mathematiker haben im 2. JH Verhältnisse als Zahlen aufgefasst, aber im Europa des 16. Und 17. JH war die Euklidische Tradition immer noch sehr stark vertreten. Newton hat als erster mit ihr gebrochen: „Unter eine \`Zahl' verstehen wir nicht einfach ein Vielfaches von Einheiten, sondern eher das abstrakte Verhältnis von einer Quantität zu einer andern Quantität [...]. Sie ist dreiartig: ganzzahlig, Verhältnis oder irrational. Eine ganze Zahl wird durch Einheit gemessen, ein Verhältnis durch den untervielfachen Teil von Einheit während eine irrationale Zahl unvergleichlich ist mit Einheit." Weiter zu den negativen Zahlen: „Grössen sind entweder positiv, d.h. grösser als Null oder negativ, d.h. weniger als Null. Zieht man in der Geometrie eine Gerade in eine Richtung, die man als positiv auffasst, so wird ihr Negatives in die andere Richtung gezeichnet." Newton schreibt, dass negative Grössen durch das Zeichen – vor der Zahl gekennzeichnet werden, positive durch ein +. Und dann gibt er Regeln fürs Multiplizieren an: „Ein Produkt ist positiv, falls seine Faktoren beide positiv sind oder beide negativ sind. Andernfalls ist es negativ." Newton gibt keine Begründungen für diese Regeln an.

Folie 121: Bestimmte Gleichungen (Descartes)

Im letzten Teil seiner Geometria stellt Descartes seine Behandlung von Gleichungen dar. Er schreibt sie immer mit Nullen auf der rechten Seite, da dies die beste Art sei, sie zu betrachten. Er findet folgende Eigenschaften:

- ist α eine Wurzel (Nullstelle, Lösung) einer Gleichung,so ist die linke Seite teilbar durch $x - \alpha$
- Eine Gleichung kann so viele positive Nullstellen haben, wie sie Wechsel von + auf – besitzt und so viele „falsch" (negative) Wurzeln wie die Anzahl von zweimal hintereinander auftretenden + oder – Zeichen.
- In jeder Gleichung kann man den zweiten Term eliminieren durch eine Substitution
- Die Anzahl der Nullstellen einer Gleichung kann gleich viel sein wie ihr Grad.

Folie 122: Descartes' Untersuchungen (Forts.)

Descartes formuliert eine Reihe von Behauptungen (die er ohne Beweis liess) über Gleichungen von 3. und 4. Grad. Kubische Gleichungen der Form

$$x^3 + ax + b = 0$$

mit rationalen Koeffizienten hat er untersucht unter der Bedingung, dass die Nullstellen reell sind. Er untersucht ihre Konstruierbarkeit durch Zirkel und Lineal. Descartes behauptet, dass es hinreichend und genügend ist, dass die Gleichung eine rationale Nullstelle besitzt. Er begründet die Notwendigkeit seiner Bedingung (wenn eine rationale Nullstelle α existiert, so klammert man $x - \alpha$ aus und erhält eine quadratische Gleichung mit rationalen Koeffizienten deren Nullstellen mit Zirkel und Lineal konstruierbar sind), jedoch nicht, dass sie hinreichend ist. Descartes hat die gleiche Frage für Quartiken betrachtet. Er behauptet, dass die Nullstellen mit Zirkel und Lineal konstruierbar sind genau dann, wenn die sogenannten kubische Resolvente (eine Hilfskubik, die Ferrari benutzt hatte in seiner Lösung der Quartik) reduzierbar ist. Descartes entdeckt auch die Methode der unbestimmten Koeffizienten, die weiter unten verwendet wird (Eulers Beweis). Diese Methode spielt eine wichtige Rolle in Algebra und Analysis (bei den Reihen).
(Siehe auch [BS] S.94).

Folie 123: Fundamentalsatz der Algebra

Descartes und Girard formulierten diese zentrale Problem der Algebra vom 18. JH. Descartes benutzte keine komplexen Zahlen und formulierte daher vorsichtig: „Jede Gleichung kann so viele verschiedene Nullstellen haben wie die Anzahl der Dimensionen der Unbekannten Grössen in der Gleichung". Girard hat 1629 in seiner *L'Invention Nouvelle en l'Algèbre* dann geschrieben, dass die Anzahl der Lösungen einer algebraischen Gleichung gleich ihrem Grad sei. Girard hat negative Zahlen und komplexe Zahlen als Nullstellen verwendet. Im 18. JH haben Mathematiker auch die folgende äquivalente Version des Fundamentalsatzes verwendet: Jedes Polynom

$$f_n(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

Mit reellen Koeffizienten kann als Produkt von linearen und quadratischen Faktoren mit reellen Koeffizienten geschrieben werden.
Erster Beweis: 1746 d'Alembert (wenig rigoros, auch für die Zeit). Im gleichen Jahr hat Euler, der grösste Mathematiker des 18. JH seinen Beweis der Berliner Akademie präsentiert. Euler hat nach einem algebraischen Beweis gesucht. Heute weiss man, dass der Satz nicht ohne den Gebrauch von Stetigkeit beweisen werden kann.

Folie 124: Beweis von Euler (10. VO)

Euler schien sich dessen bewusst gewesen zu sein. In seinem Beweis hat der die nicht-algebraischen Voraussetzungen auf ein Minimum reduziert. Er benutzte die folgenden zwei:

I. Jede Gleichung von ungeradem Grad mit reellen Koeffizienten hat mindestens eine Nullstelle.
II. Jede Gleichung von geradem Grad mit reellen Koeffizienten und negativem konstanten Term hat mindestens zwei reelle Nullstellen.

Eulers Strategie für den Rest des Beweises war, einen Prozess zu verwenden, der die Lösung einer Gleichung vom Grad $2^k m$ mit ungeradem m reduziert auf die Lösung einer Gleichung vom Grad $2^{k-1}m_1$ mit ungeradem m_1.
Euler notiert, dass es genügt, Gleichungen der Form $P_n(x) = 0$ anzuschauen für $n = 2^k$, diese seien die schwierigen. Denn falls n nicht eine Potenz von 2 sei, so finde man immer ein k mit $2^{k-1} < n < 2^k$ und dann könne man das Polynom mit $2^k - n$ Faktoren multiplizieren, etwa mit $x^{2^k - n}$ und erhalte ein Polynom vom Grad 2^k. Euler beweist den Satz für $n = 4$,8 und 16 bevor er zum allgemeinen Fall $n = 2^k$ übergeht.

Folie 125: Eulers Ansatz

Zur Illustration betrachten wir $n = 4$ und $n = 2^k$. Annahme, die Gleichung

$$x^4 + Bx^2 + Cx + D = 0$$

sei gegeben (wir können annehmen, dass die Gleichung bereits reduziert ist und keinen Term x^3 mehr enthält). Zuerst schreibt Euler die Gleichung um, mit einem Produkt

$$(x^2 + ux + \lambda)(x^2 - ux + \eta) = 0$$

Er benutzt Descartes' Methode der unbestimmten Koeffizienten und kommt auf die Gleichung

$$u^6 + 2Bu^4 + (B^2 - 4D)u^2 - C^2 = 0$$

Laut seiner Voraussetzung II hat diese Gleichung mindestens zwei reelle Nullstellen, eine davon bezeichnen wir mit u.

Folie 126: Eulers Ansatz, Forts.

Euler zeigt dann, dass die Koeffizienten λ, η in der obigen Gleichung rationale Ausdrücke in u und in den Koeffizienten (B, C, D) der ursprünglichen Gleichung sind. Als nächstes erhält Euler die gleichen Resultate, indem er allgemeine Argumente benutzt, ohne Rückgriff auf Berechnungen. Das tut er, um seine Behauptung auf beliebige Gleichungen vom Grad 2^k zu erweitern. Er benutzt dabei die folgenden (unbewiesenen) Sätze, die später eine Hauptrolle in den Theorien von Lagrange und Galois spielen:

A. Jede rationale symmetrische Funktion in den Nullstellen einer Gleichung ist eine rationale Funktion in ihren Koeffizienten (Fundamentalsatz über symmetrische Funktionen).
B. Nimmt eine rationale Funktion $\varphi(x_1, \dots, x_n)$ in den Nullstellen einer Gleichung k verschiedene Werte unter allen möglichen Permutationen der Nullstellen an, so erfüllen diese k Werte eine Gleichung vom Grad k deren Koeffizienten rationale Ausdrücke in den Koeffizienten der ursprünglichen Gleichung sind.

Folie 127: Forts.

Euler argumentiert dann: zu jeder Gleichung vom Grad n kann man n Nullstellen „zuordnen", man schreibt

$$f_n(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = (x + \alpha_1)(x + \alpha_2)\cdots(x + \alpha_n)$$

wobei $\alpha_1, \alpha_2, \cdots, \alpha_n$ gewisse Symbole sind, mit denen man operieren kann, wie wenn es gewöhnliche Zahlen wären. Die α_i sind also die negativen der Nullstellen von f_n und wir erhalten ein Gleichungssystem

$$\begin{aligned}
&\alpha_1 + \alpha_2 + \ \cdots + \ \alpha_n = a_1\\
&\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n = a_2\\
&\cdots\cdots\cdots\cdots\\
&\alpha_1\alpha_2\cdots\alpha_{n-1}\alpha_n = a_n
\end{aligned}$$

Der Fundamentalsatz der Algebra behauptet, dass α_1, α_2, ..., α_n reelle oder komplexe Zahlen sind.

Folie 128: Schritte

Euler geht beim Fall 2^k wie im Fall $n = 4$ vor. Im Fall $n = 4$ nimmt er an, dass die Gleichung vom Grad 4 mit den Koeffizienten B, C, D die Nullstellen $\alpha, \beta, \gamma, \delta$ hat. Die Nullstelle u muss dann die Summe von zwei dieser vier Nullstellen sein, kann also $\binom{4}{2} = 6$ Werte annehmen (unter allen möglichen Permutationen der Nullstellen). Daraus folgert Euler, dass u eine Gleichung vom Grad 6 erfüllen muss. Er notiert, dass die Werte von u (wegen $\alpha + \beta + \gamma + \delta = 0$) die folgenden sind:

$$\begin{array}{ll} u_1 = \alpha + \beta = p & u_4 = \gamma + \delta = -p \\ u_2 = \alpha + \gamma = q & u_5 = \beta + \delta = -q \\ u_3 = \alpha + \delta = r & u_6 = \beta + \gamma = -r \end{array}$$

die Gleichung für u ist dann von der Form

$$(u^2 - p^2)(u^2 - q^2)(u^2 - r^2) = 0$$

Das ist eine Gleichung von geradem Grad, die den konstanten Term $-p^2q^2r^2$. Um sicher zu sein, dass dieser Term negativ ist, muss man überprüfen, dass das Produkt pqr reell ist. Dazu zeigt Euler, dass

$$pqr = (\alpha + \beta)(\alpha + \gamma)(\alpha + \delta)$$

unverändert bleibt unter Permutationen der Nullstellen. Damit ist das Produkt ein rationaler Ausdruck in den Koeffizienten der Gleichung vom Grad vier mit den Koeffizienten B, C, D (von oben). Aus diesen Überlegungen kann man schliessen, dass u reell ist. Euler hat den Fall $n = 2^k$ nur skizziert. Er stellt das Polynom

$$f_n(x) = x^{2^k} + Bx^{2^k-2} + Cx^{2^k-3} + \cdots$$

vom Grad n als Produkt von zwei Faktoren vom Grad 2^{k-1} dar (wie vorher bei den Polynomen vom Grad 4):

$$(x^{2^{k-1}} + ux^{2^{k-1}-1} + \lambda x^{2^{k-1}-2} + \cdots)(x^{2^{k-1}} - ux^{2^{k-1}-1} + \eta x^{2^{k-1}-2} + \cdots)$$

und arbeitet damit weiter. Er kommt dann wie im Fall $n = 4$ auf eine Gleichung

$$(u^2 - p_1^2)(u^2 - p_2^2) \cdots (u^2 - p_N^2) = 0$$

für $2N = \binom{2^k}{2^{k-1}}$ (Euler weist nach, dass N ungerade ist), und zeigt, dass der konstante Term negativ ist (analog wie oben), woraus man schliesst, dass u reell angenommen werden kann. Die restlichen Koeffizienten (λ, μ, etc.) sind laut Euler auch rationale Ausdrücke in u und den Koeffizienten $B, C, D, \ldots$ vom Polynom $f_n(x)$.

Folie 129: Lagrange über den Beweis von Euler

Es ist unklar, auf welchen Überlegungen Euler seine Schlussfolgerungen basierte. Lagrange hat 1772 in *Sur la forme des racines imaginaire des* *équations* eine präzise Darstellung Eulers Reduktion gegeben, die die Lücken im Beweis von Euler füllt. Lagrange benutzt seine Theorie von ähnlichen Funktionen (mehr dazu vermutlich später, siehe S.100ff in [BS]), die er in seinem Werk *Réflexions sur la résolution algébriques des équations*, 1771, entwickelt hatte. Damit beweist er die Behauptung von Euler, dass die Koeffizienten λ, μ, etc. rationale Ausdrücke in u und den Koeffizienten $B, C, D, \ldots$ des Polynoms $f_n(x)$. Lagrange folgt Eulers Strategie. Andere Mathematiker des 18. JH haben in ihren Beweisen des Fundamentalsatzes Eulers Reduktion signifikant vereinfacht, seine Strategie jedoch als für gut befunden (etwa de Foncenex, 1859 oder Laplace, 1795).

Folie 130: Kritik von Gauss (Doktorarbeit 1799)

Der erste, der Eulers Formulierung des Beweises verwarf, war der junge Gauss. Seine Doktorarbeit war dem Beweis des Fundamentalsatzes gewidmet. Darin schrieb er „Da wir uns Arten der Grössen, die weder reell noch imaginär (also von der Gestalt $a + b\sqrt{-1}$) sind, ist es nicht ganz klar, wie das, was wir beweisen sollen sich von dem, was als fundamentaler Satz vermutet ist. Wenn man sich andere Formen von Grössen vorstellen könnte, etwa F, F', F'', ..., sogar dann könnte man nicht ohne Beweis annehmen, dass jede Gleichung erfüllt wird von einem reellem Wert für x oder durch einen Wert der Gestalt $a + b\sqrt{-1}$ oder durch einen Wert der Form F oder F' etc. Daher kann der Fundamentalsatz nur den folgenden Sinn haben: jede Gleichung kann entweder durch eine reelle oder durch eine komplexe Zahl der Gestalt $a + b\sqrt{-1}$ erfüllt werden oder durch einen Wert von einer bisher unbekannten Form oder durch einen Wert, der nicht in irgendeiner Form darstellbar ist. Wie diese Grössen, von denen wir keine Darstellungen kennen, diese Schatten von Schatten, addiert oder multipliziert werden, das kann in der Klarheit, die in der Mathematik nötig ist nicht formuliert werden “ (Gauss, *Werke*, Göttingen, 1866, Vol. III, pp.1-2, zitiert nach [BS]).
Ganz kurz gesagt:
„Den älteren Beweis von Jean Baptiste le Rond D’Alembert kritisierte Gauss als ungenügend, aber auch sein eigener Beweis erfüllt noch nicht die späteren Ansprüche an topologische Strenge.“ (Wikipedia, https://de.wikipedia.org/wiki/Carl_Friedrich_Gauß), laut Gauss führt die Annahme, dass Nullstellen in irgendeiner Form existieren, zu einem Zirkelschluss. Das kann man so nicht sagen – man muss zeigen, dass Nullstellen existieren, d.h. es bestand eine Lücke im Beweis von Euler/le Rond d’Alembert.

Folie 131: Restklassen modulo Polynom

1815 kommt Gauss wieder auf den Satz zurück und liefert einen Beweis, der weitgehend algebraisch ist, ohne die Existenz von Nullstellen irgendeiner Form vorauszusetzen. In dieser Version operiert Gauss mit Kongruenzen modulo einem gewissen Polynom (um die Annahme zu umgehen, dass Nullstellen existieren). Damit konstruiert er den Zerfällungskörper des ursprünglichen Polynoms. (Mehr dazu: Algebra-Lehrbücher). Kronecker hat diese Methode 1880/1881 verwendet, als er den Zerfällungskörper eines Polynoms konstruiert, ohne die Existenz der komplexen Zahlen vorauszusetzen. Unabhängig von Gauss und Kronecker hat Cauchy 1847 diesen Ansatz verwendet, um den Körper der komplexen Zahlen zu konstruieren. Dazu hat er das Polynom $x^2 + 1$ speziell betrachtet, das über $\mathbb{Q}$ irreduzibel ist (sich nicht als Produkt von zwei linearen Faktoren mit Koeffizienten in $\mathbb{Q}$ schreiben lässt), genauso wie über $\mathbb{R}$. Modulo $x^2 + 1$ ist jedes Polynom (im Ring der Polynome über $\mathbb{Q}$) kongruent zu einem linearen Polynom $ax + b$. Man kann die Elemente des Rings der Polynome über $\mathbb{Q}$ in Äquivalenzklassen modulo $x^2 + 1$ einteilen. Man schreibt jede Klasse als ein lineares Polynom in θ. D.h. man stellt die Klassen als $a\theta + b$ dar. Man kann nachprüfen, dass diese Restklassen einen Körper bilden mit der üblichen Addition und der Multiplikation

$$(a\theta + b)(c\theta + d) = (ad + bc)\theta + bd + ac\theta^2$$

(Details in Algebra-Textbüchern. Etwa Skript zur Algebra). Nun ist aber $x^2 \equiv -1$ modulo $(x^2 + 1)$, also ist $\theta^2 = -1$. Diese Multiplikation ist also die gleiche wie für komplexe Zahlen. Bemerkenswert ist, dass Euler einen algebraischen Zugang verwendet hatte, der zu Beginn des 19. JH wieder verworfen wurde, aber gegen 1880 wieder aufkam.

Folie 132: Lösen von Gleichungen mittels Radikalen

Ein weiteres Problem, das die Aufmerksamkeit der Mathematiker im 18. JH beschäftigte, war das Problem der Lösung von Gleichungen mittels Radikalen. Durch die Erfolge bei der Lösung von Gleichungen 3./4. Grades der italienischen Mathematiker motiviert, versuchten sie nun, den Grad 5 zu lösen. Viele herausragende Mathematiker arbeiteten an diesem Problem, so Tschirnhaus, Euler, Bézout, Lagrange und Vandermonde. Tschirnhaus publizierte 1683 einen Artikel in Acta Eruditorum, in dem er eine Transformation beschrieb (die sogenannte Tschirnhaus Transformation), die eine Gleichung vom Grad n

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

durch eine Substitution der Form

$$y = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$$
in eine Gleichung vom Grad n umformte:
$$y^n + c_1 y^{n-1} + \cdots + c_n = 0$$
deren Koeffizienten $c_1, c_2, \dots, c_{n-1}$ bei geeigneter Wahl der Koeffizienten $b_0, b_1, \dots, b_{n-1}$ verschwanden (es blieb dann also nur $y^n + c_n = 0$, d.h. eine 2-Term Gleichung!). Es gelang ihm, dies für Grad 3 zu beweisen und dadurch entdeckte er eine neue Methode, kubische Gleichungen zu lösen. Aus diesem Fall schloss er, dass diese Transformation für alle n möglich sei. Tschirnhaus hat seine Methode in einem Brief an Leibniz 1677 das erste Mal beschrieben. Leibniz antwortete, dass er glaube, er könne zeigen, dass für $n > 4$ die Berechnungen, die nötig waren, um die b_i zu bestimmen, nicht durchführbar seien. Nun ist es so, dass man mit einer Tschirnhaus Transformation quintische Gleichungen nicht auf 2-Term-Gleichungen reduzieren kann. Man kann sie jedoch auf eine Gleichung der Form
$$x^5 + Ax + B = 0$$
bringen (d.h. in der obigen Notation bleiben c_{n-1} und c_n). Die Koeffizienten $b_0, \dots, b_4$ sind dabei durch eine Gleichung vom Grad ≤ 3 bestimmt. Dies hatte 1786 der schwedische Historiker und Liebhaber der Mathematik E. Bring gezeigt. Hermite hat die Form mit den drei Termen 1858 benutzt, um zu zeigen, dass die Lösung der Quintik sich durch elliptische modulare Formen darstellen lässt.
Euler hat das Problem der Lösung der Quintik zweimal aufgenommen. Zuerst 1732/33 und dann 1762/73. Beide Ansätze führten nicht zu Lösungen für Gleichungen vom Grad 5 (der erste Ansatz war sogar einfach falsch, siehe [BS] S. 101f.).
Im zweiten Artikel gibt Euler zu einer allgemeinen Gleichung der Form
$$x^n = ax^{n-2} + bx^{n-3} + \cdots + q$$
Lösungen der Form
$$x = w + A\sqrt[n]{v} + B\sqrt[n]{v^2} + \cdots + Q\sqrt[n]{v^{n-1}}$$
wobei w reell ist und v eine Gleichung vom Grad $\leq n-1$ erfüllt.
Bemerkenswert an diesem Ansatz ist, dass – falls die allgemeine Gleichung mittels Radikalen (Wurzelausdrücken) lösbar ist - die Lösungen auch wirklich diese Gestalt annehmen. Abel hat dies in seinem Beweis der Unlösbarkeit der Quintik durch Wurzelausdrücke (Radikale) beweisen. Die oben stehende Gleichung für $x$war der Startpunkt von Abels Beweis.
Lagrange hat 1770/71 in *Réflections sur la résolution algébrique des équations* die Methoden zur Lösung von kubischen und quartischen Gleichungen bis zu seiner Zeit untersucht und gezeigt, warum sie alle nicht anwendbar sind bei allgemeinen Quintiken. Im weiteren benutzte er das untersuchte Material und schliesst, dass alle Methoden sich auf die Konstruktion von Hilfsgleichungen von kleinerem Grad reduzieren

(Resolventen) deren Nullstellen rationale Funktionen in den Nullstellen der zu lösenden Gleichung sind ([BS, S 103-106]).
Vandermonde hat fast zur selben Zeit ähnliche Schlüsse gezogen (*Memoir on the Solution of Equations*), wenn auch etwas weniger allgemein. Er versuchte auch, die Nullstellen von $x^n - 1 = 0$ zu bestimmen, dies gelang ihm aber nur bis $n = 11$. Seine Resultate hatten keinen Einfluss auf die Entwicklung der Algebra: sein Artikel wurde erst im 20. JH gelesen und kommentiert.

Folie 133: Unlösbarkeit der Quintik mittels Radikalen

Laut Lagrange verlangt das Problem der Lösung einer Gleichung mittels Wurzelausdrücken/Radikalen die Kenntnis der Untergruppe der Gruppe G der Permutationen ihrer Nullstellen (also die symmetrische Gruppe S_n, falls der Grad der Gleichung n ist). Ist der Grad der Gleichung n und besitzt G eine Untergruppe vom Index $k < n$, so kann die Lösung der Gleichung auf die Lösung einer (symmetrischen) Gleichung vom Grad k reduziert werden.
Lagrange konnte nicht beweisen, dass im allgemeinen eine Quintik nicht lösbar ist durch Wurzelausdrücke, da er

1. nicht wusste, dass die symmetrische Gruppe S_5 keine Untergruppen vom Index 3 oder 4 besitzt (man kann nachprüfen, dass das stimmt).
2. keinen Beweis der Tatsache hatte, dass jede Nullstelle im Zwischenschritt einer Gleichung (Nullstellen der Hilfsfunktion) eine rationale Funktion der Nullstellen der ursprünglichen Gleichung ist.

Folie 134: Zwei Richtungen (11. VO)

Nach Lagrange haben die Untersuchungen zur Lösbarkeit einer Gleichung mittels Radikalen jeweils eine der folgenden zwei Wege verwendet:

1. Untersuchungen von Gleichungen mit beliebigen (variablen) Koeffizienten deren (Galois-)Gruppe die symmetrische Gruppe S_n ist.
2. Untersuchung von Gleichungen mit numerischen Koeffizienten, um Klassen von Gleichungen von beliebigem Grad zu finden, die durch Radikale lösbar sind und um Gleichungen mit bestimmten Koeffizienten zu finden, die lösbar mit Radikalen sind.

Ruffini und Abel sind der ersten der beiden Routen gefolgt. Ruffini publiziert 1799 einen Beweis, dass die allgemeine Quintik nicht lösbar ist. Er benutzt Permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}$$

sowie Produkte von Permutationen. In seinem Beweis setzt Ruffini voraus, dass alle Nullstellen in den Zwischenschritten als Nullstellen einer Gleichung ausdrückbar sind, die eine rationale Funktion in den Wurzeln der ursprünglichen Gleichung ist. Da er dies voraussetzt und nicht beweist, hat sein Beweis eine Lücke.

Abel produzierte als Student einen „Beweis" der Lösbarkeit durch Radikale für allgemeine Quintiken. Er sah selber, dass die Arbeit fehlerhaft war. 1824 publizierte er einen kurzen Beweis der Unlösbarkeit durch Radikale der allgemeinen Quintik (so kurz, dass er beinahe unverständlich war) und im Jahr 1826 auch einen vollständigen Beweis. Dieser Beweis erschien in der ersten Ausgabe des Crelle Journal (Journal für die reine und angewandte Mathematik). Abel zeigte, dass – wenn eine quintische Gleichung lösbar ist durch Radikale – ihre Wurzeln die von Euler gefundene Form haben müssen. Er zeigte auch, dass die Wurzeln in den Zwischenschritten rationale Funktionen in den Nullstellen der ursprünglichen Gleichung sind. In seinem Beweis benutzte Abel den Satz von Cauchy, der folgendes besagt: Für $n \geq 5$ und für p die grösste Primzahl $\leq n$ hat die Gruppe S_n keine Untergruppen vom Index > 2 und $< p$. Für $n \geq 3$ hat die Gruppe S_n immer eine Untergruppe vom Index 2 (die alternierende Gruppe A_n der geraden Permutationen).

Folie 135: Aufgaben aus [ADEFSSWW]

1. (Aufgabe 5.3.1, Seite 316, eine Aufgabe von Euler, 1796) 20 Personen, Männer und Weiber, zehren in einem Wirtshause. Ein Mann verzehrt 8 Groschen, ein Weib aber 7 Groschen, und die ganze Zeche beläuft sich auf 6 Reichstaler. Nun ist die Frage, wie viel Männer und Weiber daselbst gewesen? (6 Reichstaler sind 144 Groschen)
2. (Aufgabe 5.3.5, Seite 317) Man suche zwei Zahlen, deren Produkt 105 sei, und wenn man ihre Quadrate zusammen addiert, so sei die Summe gleich 274.
3. (Aufgabe 6.2.1, Seite 371) W. Hamilton definierte die komplexen Zahlen als die Paare (x, y) mit x, y reell. Die Gleichheit zweier Zahlenpaare definierte er durch $(x, y) = (x', y')$ genau dann, wenn $x = x'$ und $y = y'$ ist. Die Addition und Multiplikation erklärte er durch $(x, y) + (x', y') = (x + x', y + y')$ und $(x, y)\times(x', y') = (xx' - yy', xy' + x'y)$. Man beweise, dass mit diesen Operationen die Menge der Zahlenpaare einen Körper bildet. Ist dieser Körper kommutativ?

Folie 136: Kapitel VII: Die Theorie der algebraischen Gleichungen im 19. JH.

Zur Erinnerung die Problemstellung: es geht um Lösungen von Gleichungen vom Grad 5 durch Radikale. Man hat etwa

$$f(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

Gibt es eine Formel, die Nullstellen dieser Gleichung aus a, b, c, d, e zu finden, indem man die üblichen Operationen (Addition, Subtraktion, Multiplikation, Division) und Wurzelziehen (bis zu 5. Wurzeln) verwendet? Nach Abel und Ruffini wissen wir, dass dies im allgemeinen nicht möglich ist. Aber wie sieht das genauer aus? Wann genau ist es möglich?

Folie 137: Zyklotomische Gleichungen

Im 19.JH gab es radikale Veränderungen in der Algebra und in andern Gebieten der Mathematik. Verschiedene Arten, Algebra zu betreiben, lösten sich ab. Ein Wendepunkt in der Entwicklung der Algebra war die Galoistheorie, deren Prototyp Gauss' Theorie der Zyklotomischen Gleichungen war. Diese Theorie diente als Ausgangpunkt für Forschungen von Abel, Galois und andern Mathematikern im 19. JH.
Als Student (in Göttingen) begann Gauss das Problem von Konstruktionen von regelmässigen Vielecken mit Zirkel und Lineal zu studieren. Dieses Problem hat eine lange Geschichte, die Geometer der Antike hatten regelmässige n-Ecke für $n = 3{,}3 \cdot 2^k, 4{,}4 \cdot 2^k, 5$ und $5 \cdot 2^k$konstruiert. Offen war die Frage, ob man ein regelmässiges 7- oder 11-Eck mit Zirkel und Lineal konstruieren könne.
Gauss hat das Problem, regelmässige Vielecke mit Zirkel und Lineal auf das Problem der Lösung der Gleichung

$$X = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$$

zurückgeführt, deren Nullstellen $x_k = e^{2\pi ik/n} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ an den Eckpunkten des regelmässigen n-Ecks sitzen.
Eulers Methode zur Lösung der Gleichung $X = 0$ von oben schauen wir im Fall $n = 7$ an.

$$\frac{x^7 - 1}{x - 1} = x^6 + x^5 + \cdots + x + 1 = 0$$

Dividiert man diese Gleichung durch x^3 und substituiert $y = x + \frac{1}{x}$, so erhält man

$$y^3 + y^2 - 2y - 1 = 0$$
Diese Gleichung hat drei Nullstellen, sagen wir $\theta_1, \theta_2, \theta_3$. Setzt man diese sukzessive in $y = x + {}^1\!/_x$ ein (umgeformt: $xy = x^2 + 1$) , so erhält man drei quadratische Gleichungen
$$x^2 - \theta_i x + 1 = 0, \qquad i = 1,2,3$$
Wenn man diese drei Gleichungen löst, erhält man die Nullstellen der Gleichung vom Grad 6.

Folie 138: Évariste Galois

Galois hat das Problem, Nullstellen von polynomialen Gleichungen zu finden, allgemein gelöst. Galois begann mit etwa 15, die Werke von Lagrange, Gauss, Cauchy und andern zu studieren[1]. Wenig später, in den Jahren 1829-31, löste Galois das Problem der Auflösbarkeit durch Wurzelausdrücke.
Über Galois kann man viel nachlesen. Der ORF hat 2010 einen spannenden Beitrag über Galois verfasst (*Der Fall Galois*, siehe Quellenangabe). Galois rebellierte ungestüm gegen Althergebrachtes, in der Mathematik, im Bildungssystem und im politischen Leben. Er kritisierte die Lehrbücher seiner Zeit (sie würden die grundlegenden Ideen verstecken hinter einer Menge von Sätzen) und die meisten Gelehrten der Akademie, sie seien vor allem an Ruhm interessiert, nicht am Fortschritt der Wissenschaft, [ADEFSSWW]. Er war Republikaner und Anhänger der Revolution von 1830 und wurde zweimal aus politischen Gründen verhaftet.
Die Mathematik war für Galois Lebensinhalt. Galois schrieb, dass die kalkülmässige Behandlung mathematischer Fragen den Fortschritt hemme ([ADEFSSWW]). Er vollzog eine Neuorientierung, die schliesslich zur Herausbildung eines strukturellen Denken führte. Galois sah die Aufgabe der Mathematiker in der Zusammenfassung der Operationen und deren Klassifikation nach ihren Schwierigkeiten und nicht nach ihrer Form. Seiner Meinung nach würden sich die umfangreichen, bis ins Detail ausgearbeiteten Kalküle dann als Spezialfälle unterordnen, die kalkülmässige Behandlung von Problemen lehnte er also nicht grundsätzlich ab (Galois, laut [ADEFSSWW]). Seine Arbeiten waren damals nicht verständlich, da er bestrebt war, sie ausserhalb der damaligen Tradition zu formulieren. Heute weiss man, dass er durchaus in der Tradition von Lagrange, Cauchy, Gauss und Abel stand. Er übernahm von ihnen die Problemstellungen und auch die Mittel zu deren Lösung.

[1] Dieser Abschnitt verwendet v.a. das Buch [ADEFSSWW].

Folie 139: Verdienste

Sein grosser Verdienst war es, die Wechselbeziehung zwischen den körpertheoretischen und den gruppentheoretischen Aspekten erkannt zu haben. Er stand am Anfang eines sich über mehr als ein Jahrhundert erstreckenden Prozesses.
Galois konnte nur wenige seiner Resultate publizieren. Er hat im Alter von 18 Jahre zwei Arbeiten zur Auflösung algebraischer Gleichungen an die Pariser Akademie geschickt. Die Arbeiten wurden in Sitzungen Ende Mai 1829 vorgelegt, gingen dann aber verloren. Eine weitere Arbeit wurde 1831 von Poisson abgelehnt. So waren zunächst nur zwei 2seitige Arbeiten und eine Arbeit *Sur la théorie des nombres* und der Brief *Lettre à Auguste Chevalier* von ihm bekannt. Erst um 1846 erschienen die Schriften von Galois, von Liouville herausgegeben, auf Drängen von Freunden und vom Bruder von Galois. Den Brief an Chevalier hatte Galois in der Nacht vor dem Duell verfasst, an dessen Verletzungen er dann starb. In diesem Brief hat Galois die wichtigsten Ergebnisse notiert, unter anderem die Auflösungstheorie.
Galois führt in seinen Arbeiten die Konzepte des Körpers (*Gebiet der Rationalität* genannt) und der Gruppe ein. Er betont, dass die Begriffe Reduzierbarkeit und Irreduzibilität einer Gleichung nur bezüglich einem Körper Sinn machen. Er sagt: „Man kann als *rational* alle rationalen Funktionen einer gewissen Anzahl bestimmter Variablen auffassen, die als bekannt vorausgesetzt sind. So kann man zum Beispiel eine gewisse Wurzel einer ganzen Zahl wählen und alle Funktionen dieser Wurzel als rational auffassen... Mit dieser Konvention werden wir jede Quantität *rational* nennen, die als rationale Funktion der Koeffizienten der Gleichung und einer gewissen Anzahl von adjungierten Quantitäten ausdrückbar ist.“
Diese adjungierten Quantitäten beeinflussen die Eigenschaften einer Gleichung und der Schwierigkeiten, mit ihr umzugehen. Die Gleichung $X = \frac{x^p-1}{x-1} = 0$, p prim, ist über dem Körper $\mathbb{Q}$ unlösbar. Wenn man zu $\mathbb{Q}$ „eine Wurzel aus einer der Hilfsgleichungen von Gauss nimmt, so zerlegt sich die Gleichung in Faktoren.“
Galois führt dann den Begriff der Gruppe von Substitutionen ein: „Substitutionen sind der Übergang von einer Permutation zu einer andern“. Er formuliert die fundamentale Eigenschaft, dass wenn zwei Substitutionen S und T in der Gruppe G sind, dass dann auch ST drin liegt.

Folie 140: Illustration

In seiner Arbeit verwendet er als `Gebiet der Rationalität' den Körper $\mathbb{Q}(a_1, \dots, a_n) =: \mathbb{Q}_0$ (die a_i sind die Koeffizienten der ursprünglichen Gleichung $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0$). Zu diesem Körper adjungiert er alle notwendigen Wurzeln der Eins. Die Gleichung

$$x^p - a = 0$$

wird mit Wurzelausdrücken lösbar, wenn man zum Bereich der Rationalität zum Beispiel die Wurzel $\sqrt[p]{a}$ adjungiert.

Folie 141: Entwicklung der Gruppentheorie im 19.JH

Der Brief von Galois an Chevalier wurde im September 1832 publiziert, er wurde jedoch nicht beachtet. Erst 1846 sammelte der berühmte Mathematiker Liouville alle Artikel von Galois (auf Anregung der Freunde und des Bruders von Galois) und publizierte sie, ergänzt mit Kommentaren, in seiner Zeitschrift *Journal des mathématiques pures et appliquées*. Damit wurde die Galoistheorie bekannt gemacht. Bereits 1856 findet sich eine eine vollständige Beschreibung der Galoistheorie in einem Buch „Kurs über höhere Algebra", sie wurde also Teil der Lehrbücher. Neben Galois haben sich auch andere Mathematiker der Zeit gruppentheoretische Methoden verwendet, zur Zeit der Publikation der Artikel von Galois waren bereits einige Sätze der Gruppentheorie bekannt. Zum Beispiel in den Resultaten von Lagrange. Auch einige von Eulers Beweisen in der Zahlentheorie weisen einen gruppentheoretischen Charakter auf. In seinen *Disquisitiones Arithmetica* (1801) hat Gauss eine Verknüpfung von binären quadratischen Formen eingeführt und damit die Verknüpfung auf Objekte angewandt, die ganz anders als Zahlen sind.

Folie 142: Binäre quadratische Formen

Eine binäre quadratische ist ein Ausdruck der Form

$$f(x, y) = ax^2 + 2bxy + cy^2$$

mit $a, b, c \in \mathbb{Z}$. Gauss nennt $D = b^2 - ac$ die *Diskriminante* der quadratischen Form. Eine wichtige Frage für Fermat, Euler und Lagrange war es, den Bereich der quadratischen Form zu bestimmen, d.h. die Menge M der ganzen Zahlen, so dass für jede ganze Zahl $N \in M$ zwei ganze Zahlen x_0, y_0 existieren mit

$$N = ax_0^2 + 2bx_0\, y_0 + cy_0^2$$

Fermat beispielsweise erhielt dazu früh schon Resultate: Er sagt, dass für $a = 1, b = 0$ und $c = 1$ (also für $x^2 + y^2$) der Bereich alle Primzahlen der Form $4n + 1$ enthält und keine Primzahl der Form $4n + 3$, dass der Bereich von $x^2 + 2y^2$ alle Primzahlen der Form $8n + 1, 8n + 3$ enthält, aber keine der Form $8n + 5$ oder $8n + 7$.

Lagrange notiert, dass, falls N durch eine solche binäre quadratische Form $f(x, y)$ wie oben darstellbar ist, so auch durch die Form f', die man durch die Substitution

$$x = \alpha x' + \beta y'$$
$$y = \gamma x' + \delta y'$$

wobei $\alpha, \beta, \gamma, \delta$ beliebige ganze Zahlen sind mit $\alpha\delta - \beta\gamma = \pm 1$. In diesem Fall gibt es eine Substitution, die invers zur obigen ist, die f' in f transformiert. Man sagt, f und f' seien *äquivalent*. Ist $\delta - \beta\gamma = 1$, so nennt eine solche Substitution eine *unimodulare* Substitution. **Gauss** nannte zwei Formen f, g, die durch eine unimodulare Substitution ineinander übergehen, *strikt äquivalent*.

Folie 143: Verknüpfung binärer quadr. Formen (12. VO)

Die Verknüpfung, die Gauss auf den binären Formen definierte, kann man so beschreiben: Sind a, b, c und a', b', c' die (ganzzahligen) Koeffizienten der beiden binären quadratischen Formen f, f' **mit der gleichen Diskriminante** D, so kann man ihre Verknüpfung $(f \oplus f')(x, y) = Ax^2 + 2Bxy + Cy^2$ wie folgt finden (Quelle: Wikipedia, https://de.wikipedia.org/wiki/Binäre_quadratische_Form):

1. Es sei $n = ggT(a, a', \frac{b+b'}{2})$
2. Man bestimme $t, u, v \in \mathbb{Z}$ mit $n = at + a'u + (\frac{b+b'}{2})v$
3. Man berechne $A := \frac{aa'}{n^2}$
4. Man berechne $B := \frac{ab't + a'bu + \frac{v(bb'+D)}{2}}{n}$
5. Man berechne $C := \frac{B^2 - D}{4A}$

(Dabei bestimmt man n, t, u, v nach dem erweiterten Euklidischen Algorithmus). (Algorithmus produziert nicht eine eindeutige Form, siehe etwa G. Pall, Kapitel 4. Man kann mit reduzierten f und f' arbeiten, das Resultat $f \oplus f'$ ist dann aber nicht automatisch reduziert). Als Beispiel: Aufgabe 1 am Ende vom Kapitel.

Gauss hat diese Verknüpfung von quadratischen binären Formen auf den strikten Äquivalenzklassen definiert, er hat gezeigt: Ist $f_3 = f_1 \oplus f_2$ und sind $f_1 \sim g_1$ und $f_2 \sim g_2$ und $g_3 = g_1 \oplus g_2$ so gilt $g_3 \sim f_3$. Er hat dann also mit den Äquivalenzklassen gerechnet. Er hat ein neutrales Element für diese Operation (auf den binären quadratischen Formen mit einer fest gewählten Diskriminante D) gefunden: ist E die Klasse von $x^2 - Dy^2$, so gilt für jede beliebige Klasse K (mit Diskriminante D) folgendes:

$$K \oplus E = E \oplus K = K$$

Er hat auch gezeigt, dass diese Verknüpfung assoziativ und kommutativ ist. (siehe auch editor's notes, Seiten 127/128 in [BS])

Folie 144: Permutationsgruppen

Eine weitere Forschungsrichtung war das Studium der Permutationsgruppen. Bereits **Lagrange** hatte gezeigt, dass die Ordnung einer Untergruppe H der symmetrischen Gruppe S_n ein Teiler von $n!$ ist (siehe Satz von Lagrange). 1815 erschien **Cauchys** „Mémoire sur le nombre de valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possible les quantités qu'elle renferme". Um die Anzahl der Werte zu bestimmen, die eine rationale Funktion $f(x_1, x_2, \dots, x_n)$ einnehmen kann unter allen möglichen Permutationen ihrer Einträge, begann er, die Theorie der Gruppen von Permutationen systematisch zu begründen. Es war das erste Mal, dass solche Gruppen als unabhängiges Objekt studiert wurden. Cauchy schrieb Permutationen in Matrixnotation als $\begin{pmatrix} a & b & c & \dots & l \\ \alpha & \beta & \gamma & \dots & \lambda \end{pmatrix}$ oder kurz einfach $\binom{A}{B}$. Er führte eine Verknüpfung

$$\binom{A}{B}\binom{B}{C} = \binom{A}{C}$$

ein und zeigt, dass $\binom{A}{A}$ die Identität ist. Mit diesem Artikel beginnt die Entwicklung der Gruppentheorie (auch wenn Cauchy den Begriff „Gruppe" noch nicht eingeführt hatte). Einige der ersten Resultate:

Cauchy zeigte (in obigem Artikel von 1815), dass jede nichtsymmetrische Funktion in n Variablen, die weniger als p Werte annimmt, für p die grösste Primzahl mit $p \leq n$, genau 2 Werte annimmt.

Bertrand zeigte, dass die Gruppe S_n für $n > 4$ keine Untergruppen hat von Index > 2 und $< n$.

Cauchy hat zwischen 1844 und 1846 folgendes wichtige Resultat gezeigt: Ist die Ordnung einer Permutationsgruppe teilbar durch die Primzahl p, so enthält sie eine Untergruppe der Ordnung p.

Sylow hat dieses Resultat 1872 verallgemeinert: ist die Ordnung einer Gruppe teilbar durch p^k, so enthält sie eine Untergruppe der Ordnung p^k. Dieser Satz ist heute als der erste Sylowsatz bekannt.

Folie 145: In Richtung Gruppentheorie

Ein Wendepunkt in der Entwicklung der Gruppentheorie war die Publikation der Arbeiten von Galois 1846. So hat **Jordan** damit angefangen, Kommentare zu den sehr kurz gehaltenen Arbeiten von Galois zu schreiben. Sein Artikel *Traité des substitutions et des équations algébriques* (Paris, 1870) war eine Zusammenfassung der Arbeit von Galois. Es war die erste vollständige und systematische Darstellung der Theorie von Substitutionsgruppen und von Anwendungen in der Geometrie, in der Theorie von elliptischen Funktionen und in der Algebra. Jordan hat keine allgemeine Definition von Gruppen benutzt. Er sagte, ein „System von Permutationen bilde eine Gruppe oder eine Garbe/ein Bündel (faisceau), falls das Produkt von zwei beliebigen Permutationen im System auch zum System gehöre". Das ist die Abgeschlossenheit unter der Operation - damit hat er eine Halbgruppe definiert. Als Beispiel hat er jedoch die Gruppe der Permutationen gebraucht und damit im Grunde genommen die Theorie von endlichen Gruppen entwickelt. Er führte Begriffe für normale Untergruppen („singuläre Untergruppen"), für einfache Gruppen, für Homomorphismen („meriedrischer Isomorphismus") und Isomorphismen („holoedrischer Isomorphismus" – „holo" von „ganz"?). Jordan zeigte, dass die Restklassen einer Gruppe bezüglich einer normalen Untergruppe auch eine Gruppe bilden (eine Quotientengruppe). Schliesslich führe er das Konzept der Kompositionsreihen ein: Ist G eine Gruppe, so findet man eine Kette von Untergruppen

$$G \supset G_1 \supset \cdots \supset G_m \supset e$$

von Untergruppen, wobei jeweils G_{i+1} normal ist in G_i. Eine solche Kette heisst Kompositionsreihe. Jordan hat gezeigt, dass für eine Gruppe G je zwei Kompositionsreihen die gleiche Anzahl Terme hat und dass die Quotientengruppen G_i/G_{i+1} der beiden Reihen die gleichen Anzahl Elemente haben (man muss sie allenfalls umnummerieren).
Hölder hat dann 1889 gezeigt, dass die Gruppen G_i/G_{i+1} in den zwei Reihen isomorph sind (nach Umordnen, falls nötig).
Cayley hat 1854 dann Gruppen abstrakt eingeführt, in einer Arbeit *On the Theory of Groups, as Depending on the Symbolic Equation* $\Theta^n = 1$. Er verlangte, dass die Gruppenoperation assoziativ ist,

$$(\alpha\beta)\gamma = \alpha(\beta\gamma)$$

solle gelten für alle α, β, γ aus der Gruppe. Er verlangte auch, dass die Multiplikation jedes Gruppenelements mit einem festen (beliebigen) Gruppenelement alle Gruppenelemente ergeben solle. Daraus ergibt sich, dass $\alpha x = \beta$ und $y\alpha = \beta$ eindeutig lösbar sind für jedes Paar α, β von Gruppenelementen.

Folie 146: Multiplikationstafel

Cayley hat seine Definition mit einer Gruppen-Multiplikationstafel illustriert.

$\cdot$	1	α	β	γ	…
1	1	α	β	γ	…
α	α	α^2	$\beta\alpha$	$\gamma\alpha$	…
β	β	$\alpha\beta$	β^2	$\gamma\beta$	…
γ	γ	$\alpha\gamma$	$\beta\gamma$	γ^2	…
…	…	…	…	…	…

Man beachte, dass jede Zeile und Spalte jedes Gruppenelement enthält. Ausserdem: die Gruppenoperation $\cdot$ muss nicht kommutativ sein, also sind $\alpha\gamma$ und $\gamma\alpha$ im Allgemeinen verschieden!
Die frühen Beispiele von Gruppen, die Cayley gab, waren alles endliche Gruppen, er gab sie mit Multiplikationstafeln und durch Erzeugende und Relationen. Er zeigte, dass es zwei verschiedene (wir sagen heute „nicht-isomorphe") Gruppen der Ordnung 4 gibt, zwei der Ordnung 6, 5 der Ordnung 8. Er zeigte auch, dass die einzige[2] Gruppe von Primzahlordnung p die zyklische Gruppe

$$\{1, \alpha, \alpha^2, \dots, \alpha^{p-1}\}$$

ist. Cayleys abstrakte Formulierung des Gruppenkonzepts war beeinflusst durch die englische Schule der symbolischen Algebra, die in den 1830ern entstanden war. Ihr gehörten z.B. Boole und Hamilton an (siehe [BS, Kapitel IX]). Cayleys Ideen wurden nicht allgemein akzeptiert. So hat etwa Jordan 1870 ausschliesslich mit Gruppen von Permutationen gearbeitet. Erleichtert wurde der Zugang zur abstrakten Gruppentheorie womöglich durch Cayleys Arbeit *The theory of groups: Graphical representation* (1878). Kurz darauf führt von Dyck den Begriff der freien Gruppe ein, deren Elemente Worte der Form $A^r B^k C^l$ … in einer Reihe von Symbolen $A, B, C, \dots$ sind. Die allgemein anerkannte Axiomatik der Gruppentheorie wurde von Weber im ersten Band eines drei-bändigen Werkes *Lehrbuch der Algebra* eingeführt. Lange Zeit war dieses Buch das Standardwerk der Algebra.

Folie 147: Siegeszug der Gruppentheorie

Das Konzept einer Gruppe – eines der wichtigsten in der modernen Mathematik – entstand allmählich aus den Forschungen in der Algebra und der Zahlentheorie. Der Fortschritt in Algebra, Analysis, Geometrie,

[2] Bis auf Isomorphie

Mechanik und der theoretischen Physik verdankt der Idee der Gruppe und zugehörigen Mengen von Invarianten sehr viel. Im Folgenden eine Liste einiger der Meilensteine dieser Entwicklungen.

1. 1870 hat Jordan alle endlichen Rotationsgruppen im 3dimensionalen Raum klassifiziert. Für die linearen Differentialgleichungen hat er ab 1871 in Analogie zur Galoistheorie eine Theorie entwickelt, in der die Rolle der Galoisgruppe einer algebraischen Gleichung durch die Monodromiegruppe der Differentialgleichung gespielt wird. Picard hat diese Theorie vervollständigt.
2. In seinem Erlanger Programm hat Klein 1872 Gruppen in der Klassifikation von Geometrien verwendet.
3. Poincaré führt das Konzept der Fundamentalgruppe in den 1880ern in die Topologie ein, Poincaré, Aleksandrov und Kolmogorov definieren Homologiegruppen.
4. In den 1880ern führt Poincaré Gruppen in der Analysis ein, um eine der wichtigsten Klasse von Funktionen zu studieren, die automorphen Funktionen. Klein und Schwarz gehen ähnlich vor.
5. Lie und Klein fangen an, die Theorie der stetigen Gruppen zu definieren. Ihre Rolle in der Theorie der partiellen Differentialgleichungen ist analog zu der Rolle von Permutationsgruppen in der Galoistheorie.
6. Jordan betrachtete schon die Theorie der Darstellungen von Gruppen durch Matrizen, eine sehr fruchtbare Idee für die weitere entwicklung der Algebra. In den 1890ern haben Molin und Frobenius eine allgemeine Theorie der Darstellungen von Gruppen entwickelt.
7. Harmonische Analysis (Differential- und Integralrechnung mit topologischen Gruppen) wurde anfänglich von Weyl entwickelt, dann von Pontrjagin.

Bald wurden Gruppen in der Physik betrachtet. Kristallographie – Klassifikation von Kristallen. Quantenphysik.

Folie 148: Aufgaben

1. Seien $f(x,y) = x^2 + y^2$ und $f'(x,y) = x^2 + 2xy + 2y^2$. Man rechne zunächst nach, dass f und von f'die gleiche Diskriminante haben, und dass sie gleich -1 ist. Dann berechne man nach dem Algorithmus von Gauss (einen Repräsentant für) die Form $f \oplus f'$ und ihre Diskriminante.

2. Wenn man als Gruppe $G = \mathbb{Z}$ die ganzen Zahlen nimmt, so ist jede Untergruppe ein Normalteiler (da $\mathbb{Z}$ kommutativ ist). Die Untergruppen von $\mathbb{Z}$ sind die Mengen der Vielfachen von einer gegebenen Zahl, also $m\mathbb{Z}$ ($m \geq 0$). Man schaue sich $\mathbb{Z}/6\mathbb{Z}$ an und überzeuge sich, dass das eine Gruppe ist – dass $\mathbb{Z}/6\mathbb{Z}$ ein neutrales Element hat, dass das Halbgruppenkriterium von Jordan gilt und dass jedes Element ein (additives) Inverses besitzt.
3. ([K], Aufgabe 2, Seite 759). Für die Primzahl $p = 7$ berechne man für jede ganze Zahl $1 < a < p$ den kleinsten Exponenten m mit der Eigenschaft, dass $a^m \equiv 1$ (modulo 7).
4. ([K], Aufgabe 2, Seite 759). Es sei p prim und $0 < a < p$, es sei m der kleinste Exponent mit $a^m \equiv 1$ (modulo p). Man zeige, dass m ein Teiler von $p - 1$ ist.