Algebra I/II – HS 2017/FS 2018

E. Kowalski (Algebra I)
M. Burger (Algebra II)

September 20, 2017

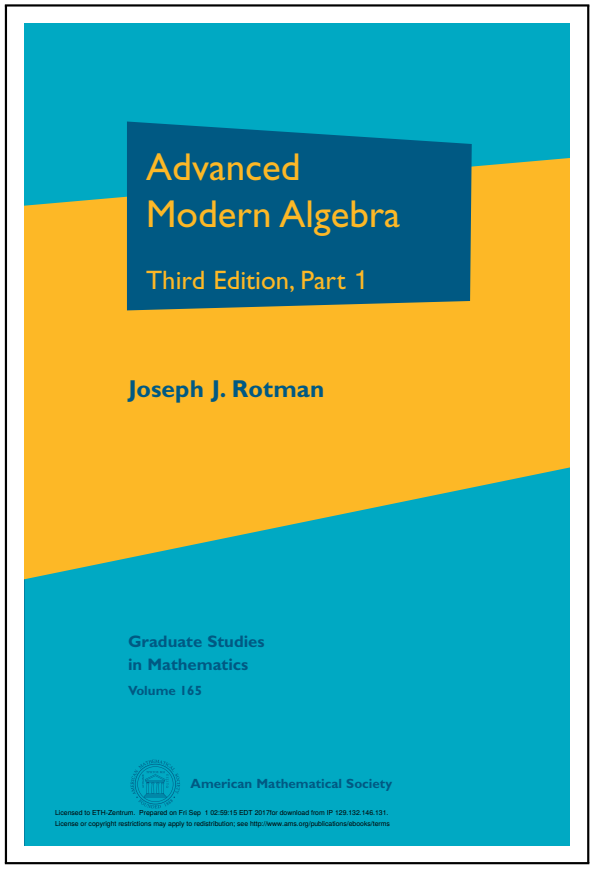
Information

- **Lectures.** HG E5, Wednesdays, 13–15 and Fridays, 8–10.
- **Home page:**
  `https://metaphor.ethz.ch/x/2017/hs/401-2003-00L/`
- **Exercise classes.** Mondays 14–16 (one class on Wednesdays, 15–17), see home page.
- **Exercise sheets.** New exercise sheet posted on Fridays on the home page; prepare question over the week-end for the next exercise class; hand in solutions by next Friday at 12:00 in HG J 68.

Exam

- **Math bachelor students**: oral exam for Algebra I/II in August 2018 (30 minutes).
- **Important:** for other students, exams are separate in February 2018 and August 2018 (20 minutes each). It is possible to register for a single combined exam, but not in `myStudies`, only directly through the examination office.
- **Midterm.** An *optional* mid-term exam for Algebra I will be organized the first day of the Spring semester. In case the grade in the midterm is better than the grade of the oral exam, it will be counted for 20%.

References



Main reference: *Advanced Modern Algebra* by J. Rotman (third edition, part 1).

Available online at `http://www.ams.org/books/gsm/165/`

For certain parts, additional material will be written by the professor (e.g., group actions).

A quick historical overview

- **Algebra**: from the latin *algebra*, from the arabic *al-jabr*, "the restoration of broken parts" (also used in surgery in the treatment of fractures), from the title of the book *al-kitāb al-mukṯaṣar fī ḥisāb al-jabr wal-muqābala* by al-Ḵwārizmī (from whose name the word "algorithm" also comes), written around 830.
- This refers to the operation of bringing an expression such as $x^2 = 4x - x^2$ to the equivalent form $2x^2 = 4x$ by adding x^2 on both sides.

(continued)

Important dates:

- Italian renaissance (solution of the cubic and quartic equations, first hints of Galois theory).
- Leibniz (formalism of differential calculus).
- 18th/19th century: evolution of linear algebra.
- 19th century: É. Galois (group theory and Galois theory).
- Early 20th century: foundations of modern algebra (D. Hilbert and E. Noether in particular).

A comparison

Now it has been seen above that each set of n a's which have the same second suffix are transformed among themselves by every substitution of the group. Hence for each j the set of s linear functions

$$\sum_{i=1}^{i=n} C_{ij}^{(k)} a_{ij} \quad (k = 1, 2, \ldots, s)$$

are transformed among themselves by every substitution of the group. If for any second suffix j which actually occurs this set of s functions is linearly equivalent to $r\ (< n)$, then a set of r linear functions of

$$a_{1j},\ a_{2j},\ \ldots,\ a_{nj}$$

exists which are transformed among themselves; and therefore there is a corresponding set of r linear functions of the x's which are transformed among themselves by the substitutions of G, *i.e.*, G is reducible.

If for each second suffix that occurs the s functions were equivalent to n (in which case s must be a multiple of n), successive sets of symbols with the same second suffix might be eliminated from equations (ii) till there remain only n equations. These may be brought to the form

$$\left.\begin{aligned} \beta_{1j_1} + B_{1j_2} + \ldots &= 0 \\ \beta_{2j_1} + B_{2j_2} + \ldots &= 0 \\ \ldots \quad\quad \ldots \quad\quad &\ldots \\ \beta_{nj_1} + B_{nj_2} + \ldots &= 0 \end{aligned}\right\}, \qquad \text{(iv)}$$

where $B_{1j_2}, B_{2j_2}, \ldots, B_{nj_2}$ are n linearly independent functions of

$$\beta_{1j_2},\ \beta_{2j_2},\ \ldots,\ \beta_{nj_2}.$$

Now, in the group on the n^2 variables, symbols with the same second suffix are transformed among themselves. Hence, if A_{rj_2} is the same function of $a_{1j_2}, a_{2j_2}, \ldots, a_{nj_2}$ that B_{rj_2} is of the corresponding β's, then

$$\begin{aligned} &a_{1j_1} + A_{1j_2} + \ldots, \\ &a_{2j_1} + A_{2j_2} + \ldots, \\ &\ldots \quad\quad \ldots \quad\quad \ldots \\ &a_{nj_1} + A_{nj_2} + \ldots \end{aligned}$$

are transformed among themselves, and therefore $a_{1j_1}, a_{2j_1}, \ldots, a_{nj_1}$ and $A_{1j_2}, A_{2j_2}, \ldots, A_{nj_2}$ undergo the same transformation for every substitution of the group.

Hence also $\quad a_{1j_2},\ a_{2j_2},\ \ldots,\ a_{nj_2}$

and $\quad A_{1j_2},\ A_{2j_2},\ \ldots,\ A_{nj_2}$

2. Unter einem *Ideal* $\mathfrak{M}$[8]) in Σ werde ein System von Elementen aus Σ verstanden, das den beiden Bedingungen genügt:

1. $\mathfrak{M}$ *enthält neben* f *auch* $a \cdot f$, *wo* a *ein beliebiges Element aus* Σ *ist.*

2. $\mathfrak{M}$ *enthält neben* f *und* g *auch die Differenz* $f - g$; also neben f auch $n f$ für jede ganze Zahl n.

Ist f Element von $\mathfrak{M}$, so drücken wir das wie üblich durch $f \equiv 0\,(\mathfrak{M})$ aus; und sagen, f *ist durch* $\mathfrak{M}$ *teilbar*. Ist jedes Element von $\mathfrak{N}$ zugleich Element von $\mathfrak{M}$, also teilbar durch $\mathfrak{M}$, so sagen wir: $\mathfrak{N}$ *ist durch* $\mathfrak{M}$ *teilbar*; in Zeichen: $\mathfrak{N} \equiv 0\,(\mathfrak{M})$. $\mathfrak{M}$ heißt *echter Teiler* von $\mathfrak{N}$, wenn es von $\mathfrak{N}$ verschiedene Elemente enthält, also nicht umgekehrt durch $\mathfrak{N}$ teilbar ist. Aus $\mathfrak{N} \equiv 0\,(\mathfrak{M})$; $\mathfrak{M} \equiv 0\,(\mathfrak{N})$ folgt $\mathfrak{N} = \mathfrak{M}$.

Auch die übrigen bekannten Begriffe bleiben wörtlich erhalten. Unter dem *größten gemeinsamen Teiler* zweier Ideale $\mathfrak{A}$ und $\mathfrak{B}$ — $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$ — verstehen wir die Gesamtheit der Elemente, die sich in der Form $a + b$ darstellen lassen, wo a alle Elemente aus $\mathfrak{A}$, b alle aus $\mathfrak{B}$ durchläuft; $\mathfrak{D}$ wird wieder ein Ideal. Ebenso ist der größte gemeinsame Teiler von unendlich vielen Idealen — $\mathfrak{D} = (\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\nu, \ldots)$ — definiert als Gesamtheit der Elemente d, die sich darstellen lassen als Summe der Elemente von jeweils endlich vielen Idealen: $d = a_{i_1} + a_{i_2} + \ldots + a_{i_n}$; auch hier wird $\mathfrak{D}$ wieder ein Ideal.

Enthält das Ideal $\mathfrak{M}$ insbesondere eine endliche Anzahl von Elementen $f_1, f_2, \ldots, f_\varrho$ derart, daß

$$\mathfrak{M} = (f_1 \ldots f_\varrho); \quad \text{d. h.} \quad f = a_1 f_1 + \ldots + a_\varrho f_\varrho + n_1 f_1 + \ldots + n_\varrho f_\varrho$$

wird für jedes $f \equiv 0\,(\mathfrak{M})$, wobei die a_ι Größen des *Ringbereiches*, die n_ι ganze Zahlen sind, so wird $\mathfrak{M}$ als *endliches Ideal* bezeichnet; $f_1, \ldots, f_\varrho$ als eine *Idealbasis*.

Wir legen nun im folgenden nur *solche Ringe* Σ *zugrunde, die die Endlichkeitsbedingung erfüllen: Jedes Ideal in* Σ *ist ein endliches, besitzt also eine Idealbasis.*

3. Aus der Endlichkeitsbedingung folgt direkt der allen folgenden Überlegungen zugrunde liegende

Satz I (*Satz von der endlichen Kette*)[9]): *Ist* $\mathfrak{M}, \mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_\nu, \ldots$

[8]) Ideale werden mit großen deutschen Buchstaben bezeichnet. $\mathfrak{M}$ soll an das Beispiel des gewöhnlich als „Modul" oder Formenmodul bezeichneten Ideals aus Polynomen erinnern. Übrigens benutzen die §§ 1—3 nur die Modul- und nicht die Idealeigenschaft; vgl. dazu § 9.

[9]) Zuerst ausgesprochen für Zahlenmoduln von Dedekind: Zahlentheorie, Suppl. XI, § 172, Satz VIII (4. Auflage); unser Beweis und die Bezeichnung „Kette" ist von dort übernommen. Für Ideale aus Polynomen bei Lasker, a. a. O. S. 56 (Hilfssatz). Der Satz findet aber in beiden Fällen nur vereinzelte Anwendung. Unsere Anwendungen beruhen durchweg auf dem *Auswahlpostulat.*