Des calculs aux résultats : éléments de genèse des treillis chez Dedekind

Emmylou Haffner

Institut de Mathématique d'Orsay, Université Paris Saclay

Séminaire itinérant du Centre d'Alembert, 23 novembre 2020

Le produit de tous les nombres plus petits qu'un nombre premier étant augmenté de l'unité, est divisible par ce nombre premier, a été publié par Waring qui l'attribue à Wilson (Meditationes Algeb. Ed. 5, p. 380); mais aucun des deux n'a pu le démontrer, et Waring avoue que la démonstration lui en semble d'autant plus difficile qu'il n'y a point de notation par laquelle on puisse exprimer un nombre premier; pour nous, nous pensons que la démonstration de cette sorte de vérités doit être puisée dans les notions [notionibus, traduit en allemand par Begriffen] plutôt que dans la notation.

(Gauss, *Disquisitiones Arithmeticae*, 1801, trad. fr. 1807, 56)

[C]ette base de la théorie, bien qu'elle ne laisse rien à désirer du côté de la rigueur, n'est nullement celle que je me propose d'établir. On peut remarquer, en effet, que les démonstrations des propositions les plus importantes se sont appuyées sur (. . .) un calcul qui coïncide avec la composition des formes quadratiques binaires, enseignée par Gauss. Si l'on voulait traiter de la même manière tous les corps Ω de degré quelconque, on se heurterait à de grandes difficultés, peut-être insurmontables. Mais, lors même qu'il n'en serait pas ainsi, une telle théorie, fondée sur le calcul, n'offrirait pas encore, ce me semble, le plus haut degré de perfection ; il est préférable, comme dans la théorie moderne des fonctions, de chercher à tirer les démonstrations, non plus du calcul, mais immédiatement des concepts fondamentaux caractéristiques, et d'édifier la théorie de manière qu'elle soit, au contraire, en état de prédire les résultats du calcul (par exemple, la composition des formes décornposables de tous les degrés).

(Richard Dedekind, 1876-77, "Théorie des nombres entiers algébriques", *Bulletin des Sciences Astronomiques et Mathématiques*, 1876-1877, 102)

The legend according to which Riemann found his mathematical results through grand general ideas without requiring the formal tools of analysis, is not as widely believed today as it was during Felix Klein's lifetime. Just how strong Riemann's analytic technique was is especially clearly shown by the derivation and transformation of his asymptotic series for $\zeta(s)$.

(Carl Siegel, 1932, Über Riemanns Nachlass zur analytischen Zahlentheorie, *Gesammelte Werke* I, 276)

> *Surely a mathematician of Riemann's greatness would want to simplify and organize his formulas in the clearest possible way, but to say that Riemann would insist that Darstellungsformen should always be results, not tools, of the theory is, I believe, a serious misrepresentation. (. . .) He was, rather, a virtuoso of Darstellungsformen.*

(Harold Edwards, 2010, The Algorithmic Side of Riemann's Mathematics, *A Celebration of the Mathematical Legacy of Raoul Bott*, 63)

- Des calculs derrière les concepts ?
- Dedekind : des calculs mais également une grande attention aux notations et manières de présenter.
- Les mathématiques conceptuelles à cette époque : une caractérisation des textes publiés plus que des pratiques ?
- Publications et brouillons, “the front and the back of mathematics” ? (cf. Hersch, Mathematics has a front and a back. *Synthese*, 1991)
- Comment écrire les mathématiques ‘terminées’ vs. comment sont écrites les mathématiques *en train de se faire*.

Les *Dualgruppen* de Dedekind

> *Pendant de nombreuses années, j'ai été occupé par ces questions, mais je n'y ai pas été poussé par la logique, mais par la théorie de ces systèmes de nombres que j'appelle modules. Par mes efforts pour obtenir cette théorie à partir du plus petit nombre de lois fondamentales, et non sans grandes difficultés, j'ai reconnu les [propriétés définissant les Dualgruppen] (...)*

(Richard Dedekind, Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler, 1897)

Les modules

Un système $\mathfrak{a}$ de nombres réels ou complexes α, dont les sommes et différences appartiennent aussi à $\mathfrak{a}$, sera appelé un module.

"Über die Composition der binären quadratische Formen, Xth Supplement". In Dirichlet, L. Vorlesungen über Zahlentheorie, 1871.

- Un module $\mathfrak{a}$ est divisible par un module $\mathfrak{b}$ ssi $\mathfrak{a} \subset \mathfrak{b}$.
- Le Plus Petit Commun Multiple de 2 modules $\mathfrak{a}, \mathfrak{b}$ est leur intersection.
- Le Plus Grand Commun Diviseur de $\mathfrak{a}$ et $\mathfrak{b}$ est le module composé par tous les nombres $\alpha + \beta$ avec α et β parcourant respectivement tous les nombres de $\mathfrak{a}$ et $\mathfrak{b}$.

Dans "*Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers*" (1877), Dedekind introduit des symboles pour être multiple ($>$), être diviseur ($<$), le PPCM ($-$), et le PGCD ($+$) de modules.

Pour des modules $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ avec $\mathfrak{a} < \mathfrak{b}$:

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c}))$$

$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c}))$$

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = (\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c})$$

ou encore

$$\mathfrak{a} + (\mathfrak{b} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + \mathfrak{c})$$

dans lesquels on remarque un « dualisme particulier entre le PPCM et le PGCD ».

- Dedekind, R. (1897). Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler. *Festschrift der Technischen Hochschule zu Braunschweig bei Gelegenheit der 69. Versammlung Deutscher Naturforscher und Ärzte,* 1–40. Repr. in (Dedekind, 1932) II, 103-147.
- Dedekind, R. (1900). Über die von drei Moduln erzeugte Dualgruppe. *Mathematische Annalen,* 53, 371-403. Repr. in (Dedekind, 1932) II, 236–271.

Un système $\mathfrak{A}$ de choses $\alpha, \beta, \gamma, \ldots$ est appelé un Dualgruppe, s'il existe deux opérations $\pm$, telles que de deux choses α, β, elles créent deux choses $\alpha \pm \beta$, qui sont aussi dans $\mathfrak{A}$ et qui satisfont

$$\begin{array}{cc} \alpha + \beta = \beta + \alpha & \alpha - \beta = \beta - \alpha \\ (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) & (\alpha - \beta) - \gamma = \alpha - (\beta - \gamma) \\ \alpha + (\alpha - \beta) = \alpha & \alpha - (\alpha + \beta) = \alpha \end{array}$$

- Une relation d'ordre (partielle) : $\mathfrak{a} < \mathfrak{b}$ (a divise b) (ou $\mathfrak{b} > \mathfrak{a}$), la relation de divisibilité qu'on peut aussi définir comme $\mathfrak{a} < \mathfrak{b}$ (a div b) ssi $\mathfrak{a} + \mathfrak{b} = \mathfrak{a}$.
- Une loi appelée *Modulgesetz* (loi modulaire) : pour $\mathfrak{d}, \mathfrak{m}, \mathfrak{p}$ modules avec $\mathfrak{d} < \mathfrak{m}$, alors
$$(\mathfrak{m} + \mathfrak{p}) - \mathfrak{d} = \mathfrak{m} + (\mathfrak{p} - \mathfrak{d})$$
- Le *Dualgruppe* est un concept général pour lequel on peut trouver de nombreux exemples, de nombreuses applications : la logique de Schröder, les modules, les idéaux, les groupes abéliens infinis, les groupes de Galois, les corps, certains espaces de nombres...

La genèse des *Dualgruppen*

- Dans les brouillons de Dedekind : exploration des et expérimentations sur propriétés des modules et leurs opérations par les calculs.
- Généralisation progressive : exemples numériques, cas particuliers simples, cas particuliers plus généraux, résolution de problèmes, tentatives de généralisation...
- Observation des propriétés et lois vérifiées par les opérations, identification des lois générales, des lois fondamentales...
- Processus non linéaire : phases de recherche et de textualisation s'entrecoupent et se répètent.

- Niedersächsische Staats- und Universitätsbibliothek Göttingen : Cod. Ms. R. Dedekind, III 14, X 9, X 10, X 11-1, X 11-2, XI 1, XI 2, XI 3-1 et XI 3-2.
- Édition des brouillons : `http://eman-archives.org/Dedekind/`

La genèse des *Dualgruppen*

- Dans les brouillons de Dedekind : exploration des et expérimentations sur propriétés des modules et leurs opérations par les calculs.
- Généralisation progressive : exemples numériques, cas particuliers simples, cas particuliers plus généraux, résolution de problèmes, tentatives de généralisation...
- Observation des propriétés et lois vérifiées par les opérations, identification des lois générales, des lois fondamentales...
- Processus non linéaire : phases de recherche et de textualisation s'entrecoupent et se répètent.

- Niedersächsische Staats- und Universitätsbibliothek Göttingen : Cod. Ms. R. Dedekind, III 14, X 9, X 10, X 11-1, X 11-2, XI 1, XI 2, XI 3-1 et XI 3-2.
- Édition des brouillons : `http://eman-archives.org/Dedekind/`

Les calculs

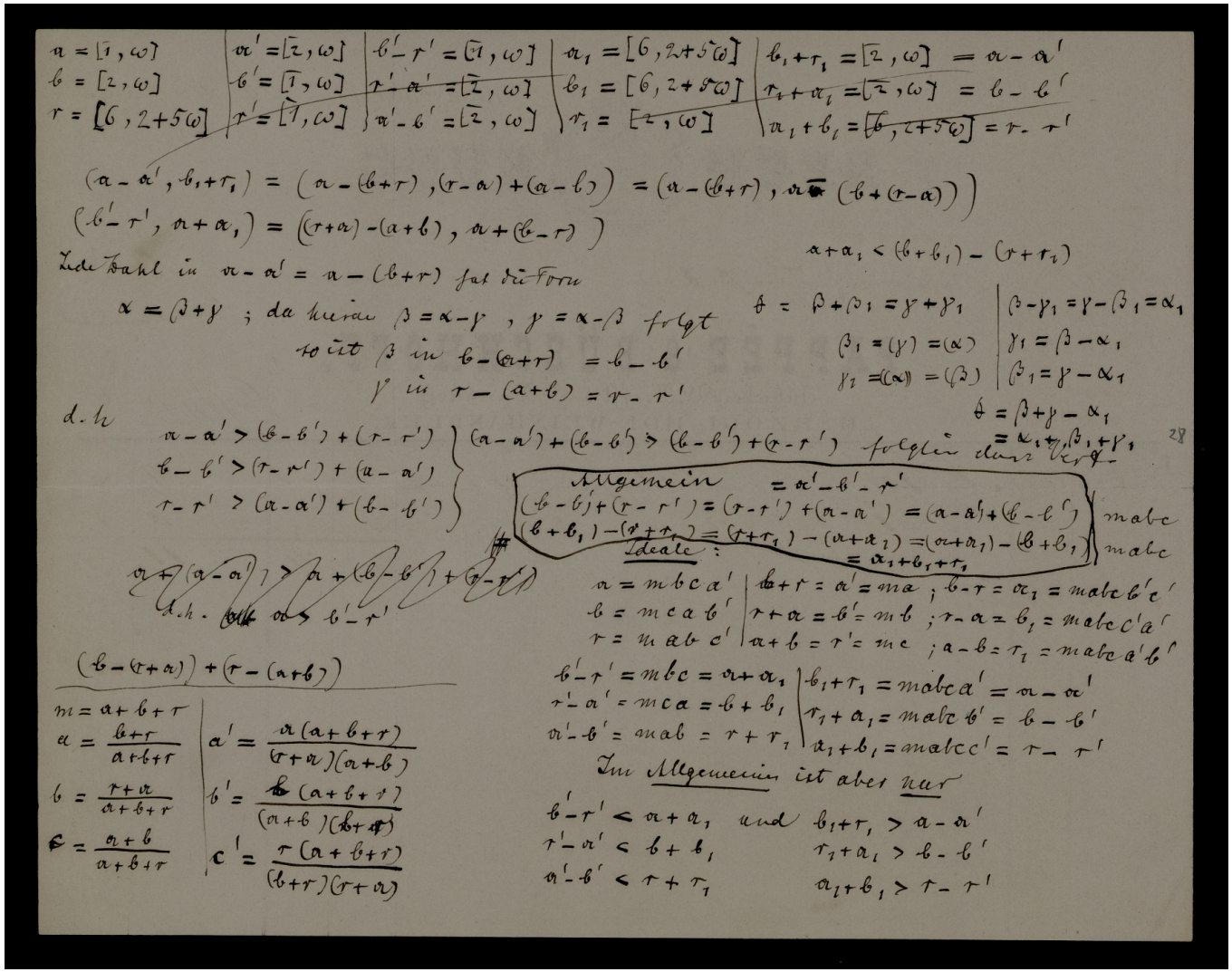


Figure: Cod. Ms. Dedekind X 11-1, p.39r.

Les notations

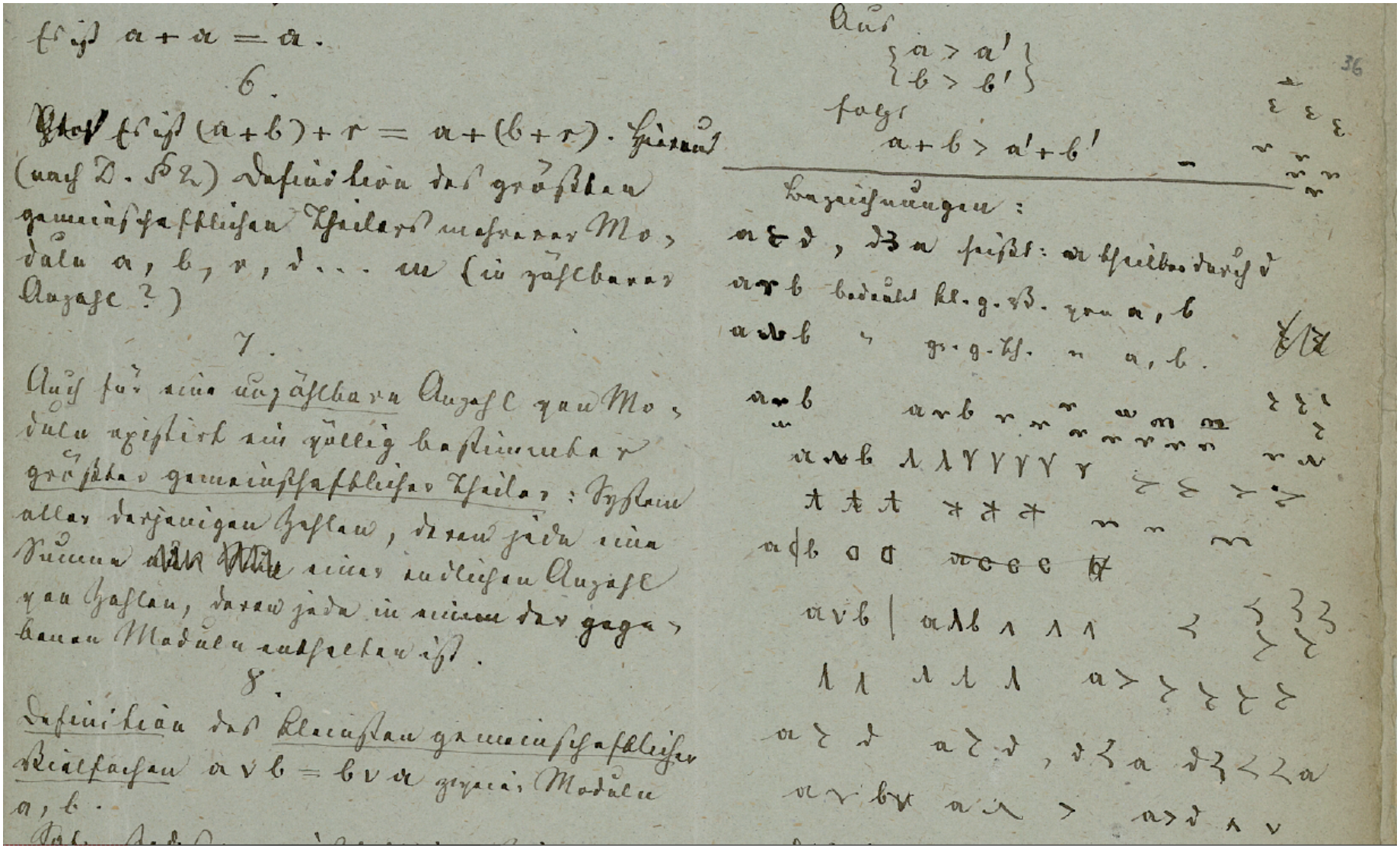


Figure: Cod. Ms. Dedekind XI-1, p.36r.

Pour trois modules $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$:

$$\begin{array}{rl} \textit{Plus grand} \\ \textit{commun} \\ \textit{diviseur} \end{array} \left\{ \begin{array}{l} \mathfrak{a}' = \mathfrak{b} + \mathfrak{c} \\ \mathfrak{b}' = \mathfrak{c} + \mathfrak{a} \\ \mathfrak{c}' = \mathfrak{a} + \mathfrak{b} \end{array} \right. \qquad \begin{array}{rl} \textit{Plus petit} \\ \textit{commun} \\ \textit{multiple} \end{array} \left\{ \begin{array}{l} \mathfrak{a}_1 = \mathfrak{b} - \mathfrak{c} \\ \mathfrak{b}_1 = \mathfrak{c} - \mathfrak{a} \\ \mathfrak{c}_1 = \mathfrak{a} - \mathfrak{b} \end{array} \right.$$

(Cod. Ms. Dedekind X 11-1, p. 19v)

Puis

$$\begin{array}{c} \mathfrak{a}_2 = \mathfrak{a} + \mathfrak{a}_1 \\ \mathfrak{a}'' = \mathfrak{a} - \mathfrak{a}' \\ \mathfrak{a}_3 = \mathfrak{b}_1 + \mathfrak{c}_1 \\ \mathfrak{a}''' = \mathfrak{b}' - \mathfrak{c}' \end{array}$$

etc.

$$\text{I. } (\mathfrak{b}-\mathfrak{b}')+(\mathfrak{c}-\mathfrak{c}')=(\mathfrak{c}-\mathfrak{c}')+(\mathfrak{a}-\mathfrak{a}')=(\mathfrak{a}-\mathfrak{a}')+(\mathfrak{b}-\mathfrak{b}')$$
$$=(\mathfrak{a}-\mathfrak{a}')+(\mathfrak{b}-\mathfrak{b}')+(\mathfrak{c}-\mathfrak{c}')=\mathfrak{a}'-\mathfrak{b}'-\mathfrak{c}'$$

$$\text{II. } (\mathfrak{b}+\mathfrak{b}_1)-(\mathfrak{c}+\mathfrak{c}_1)=(\mathfrak{c}+\mathfrak{c}_1)-(\mathfrak{a}+\mathfrak{a}_1)=(\mathfrak{a}+\mathfrak{a}_1)-(\mathfrak{b}+\mathfrak{b}_1)$$
$$=(\mathfrak{a}+\mathfrak{a}_1)-(\mathfrak{b}+\mathfrak{b}_1)-(\mathfrak{c}+\mathfrak{c}_1)=\mathfrak{a}_1+\mathfrak{b}_1+\mathfrak{c}_1$$

Les tableaux

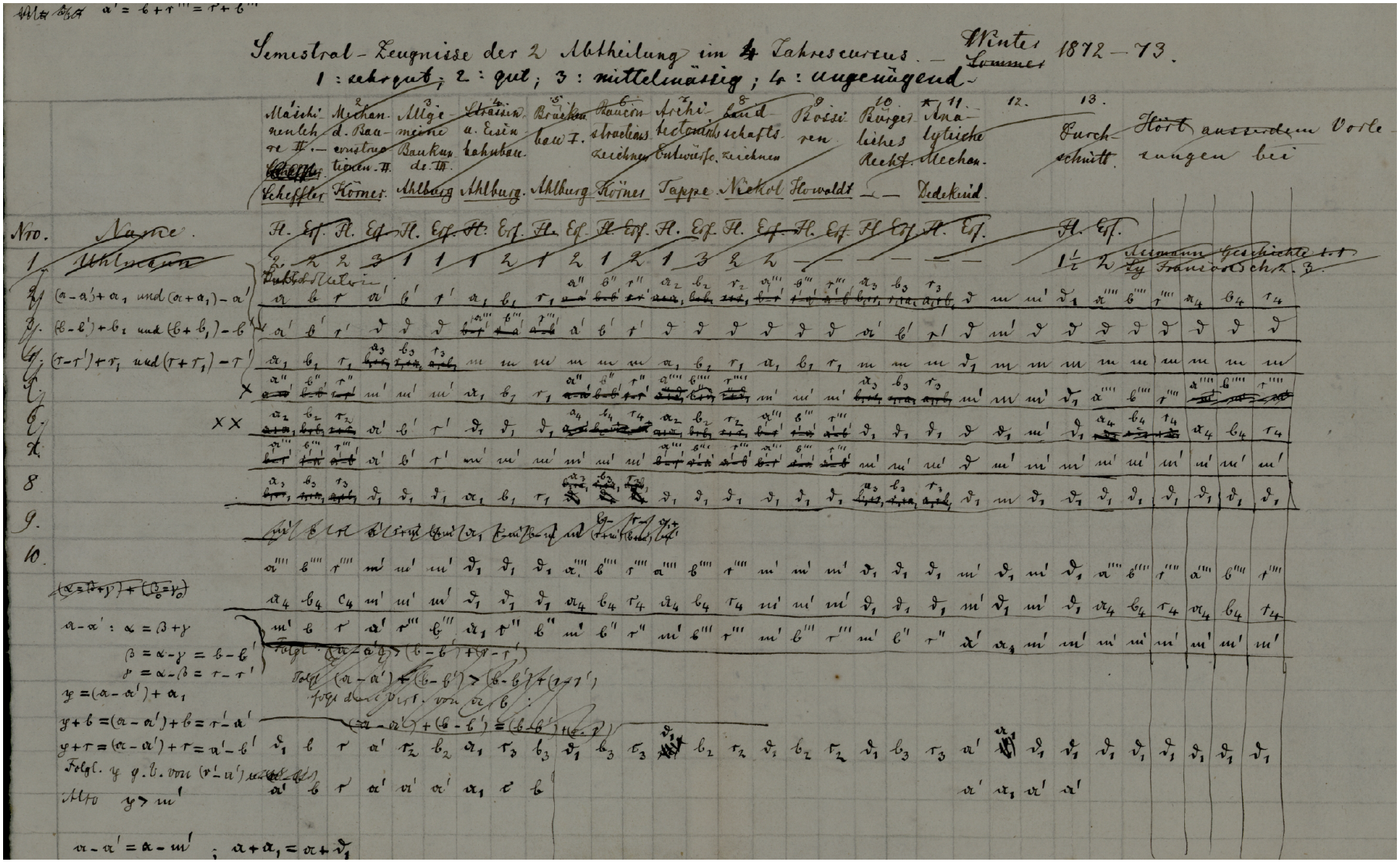


Figure: Cod. Ms. Dedekind X 11-1, p.18v.

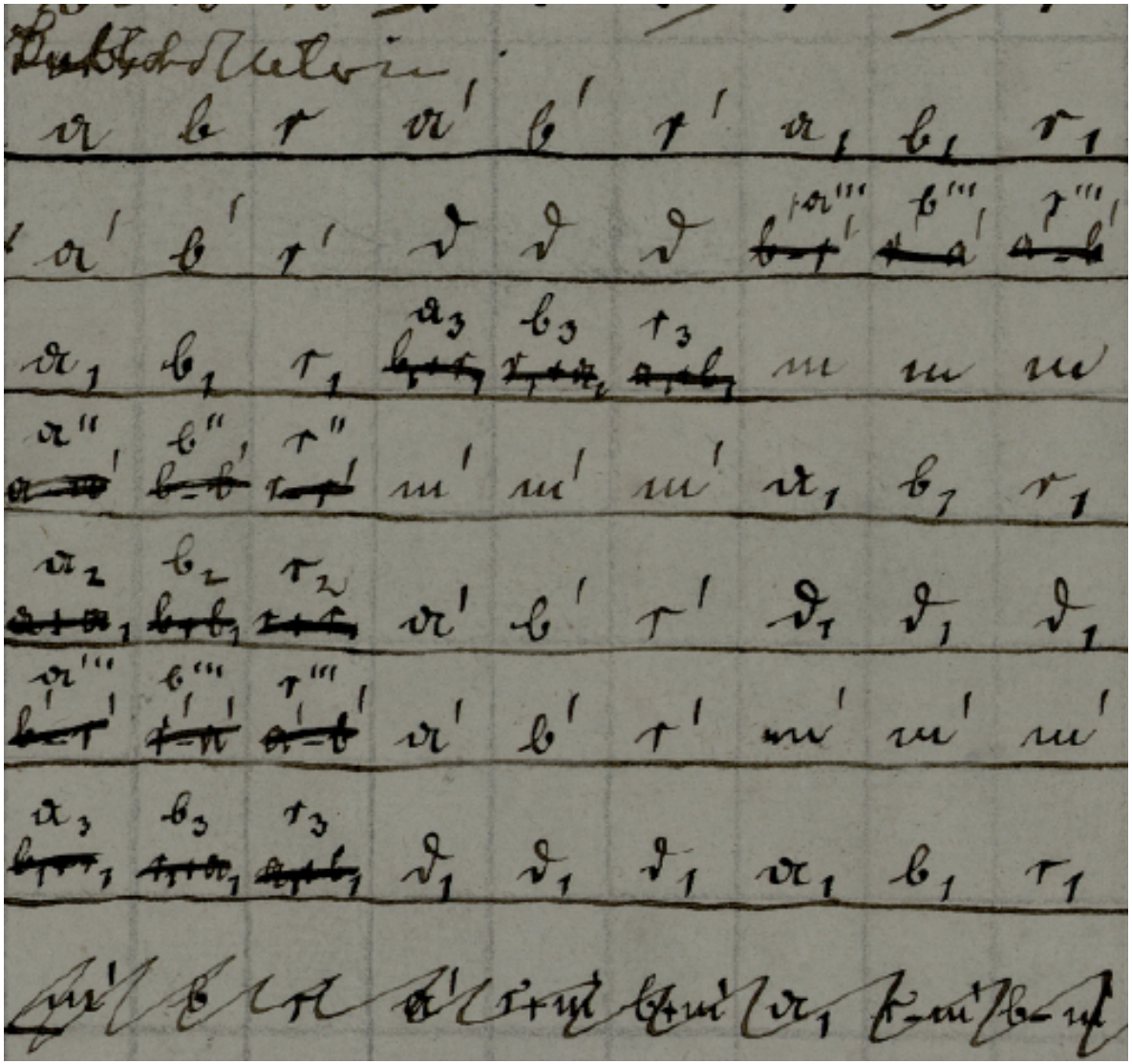


Figure: Zoom sur une partie de Cod. Ms. Dedekind X 11-1, p.18v.

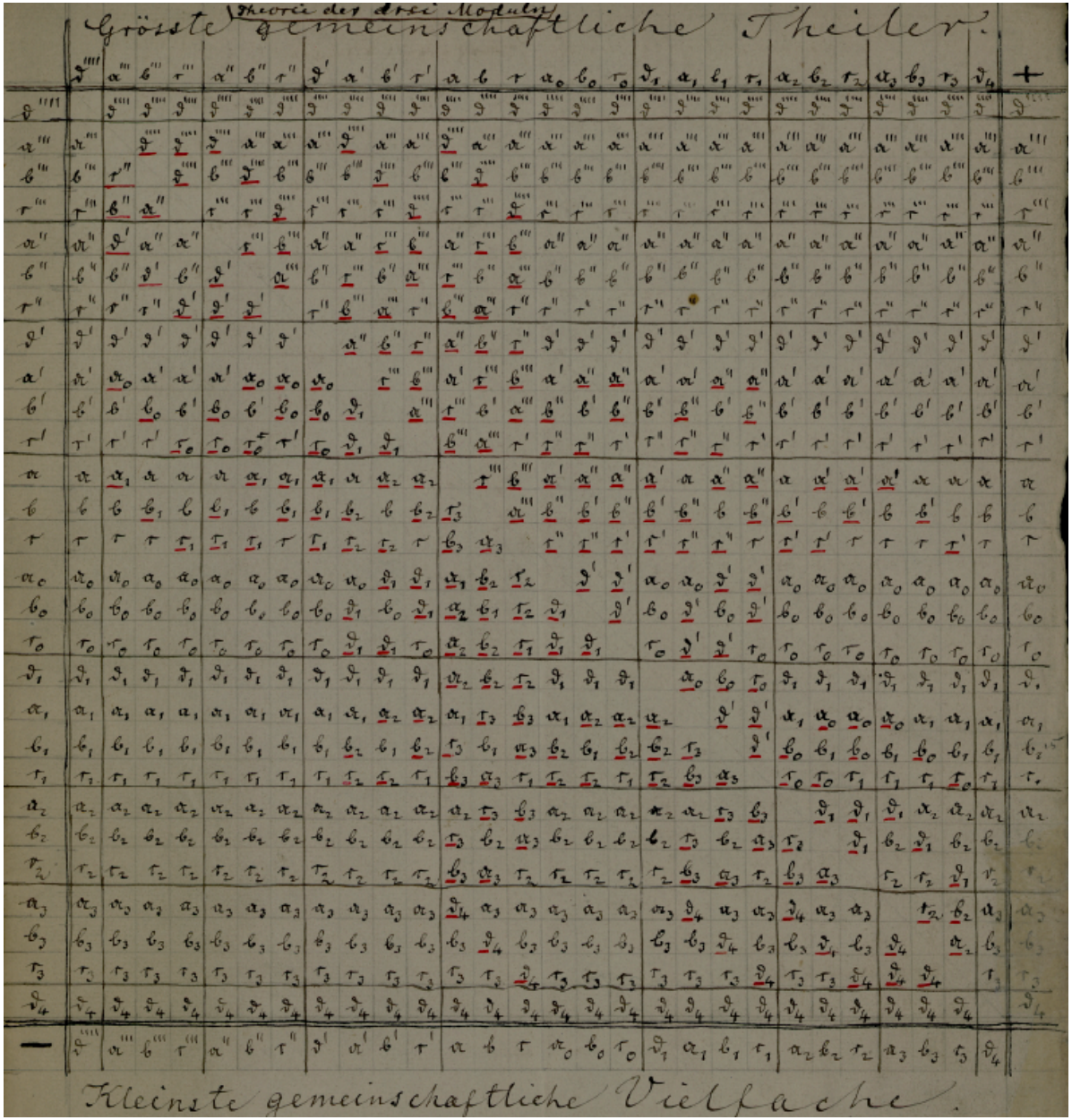


Figure: Cod. Ms. Dedekind X 11-2, p. 15r.

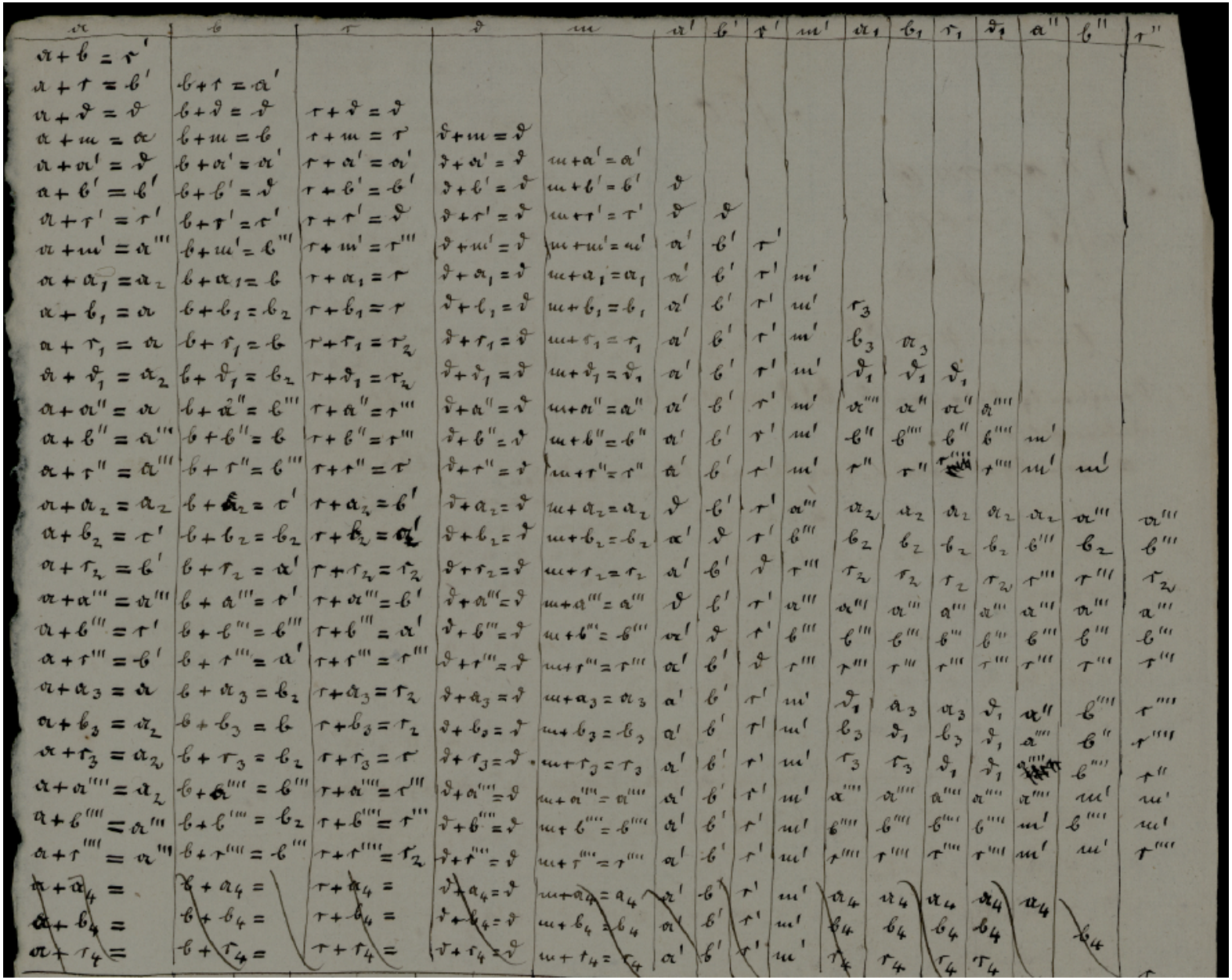


Figure: Cod. Ms. Dedekind X 11-1, p. 26v.

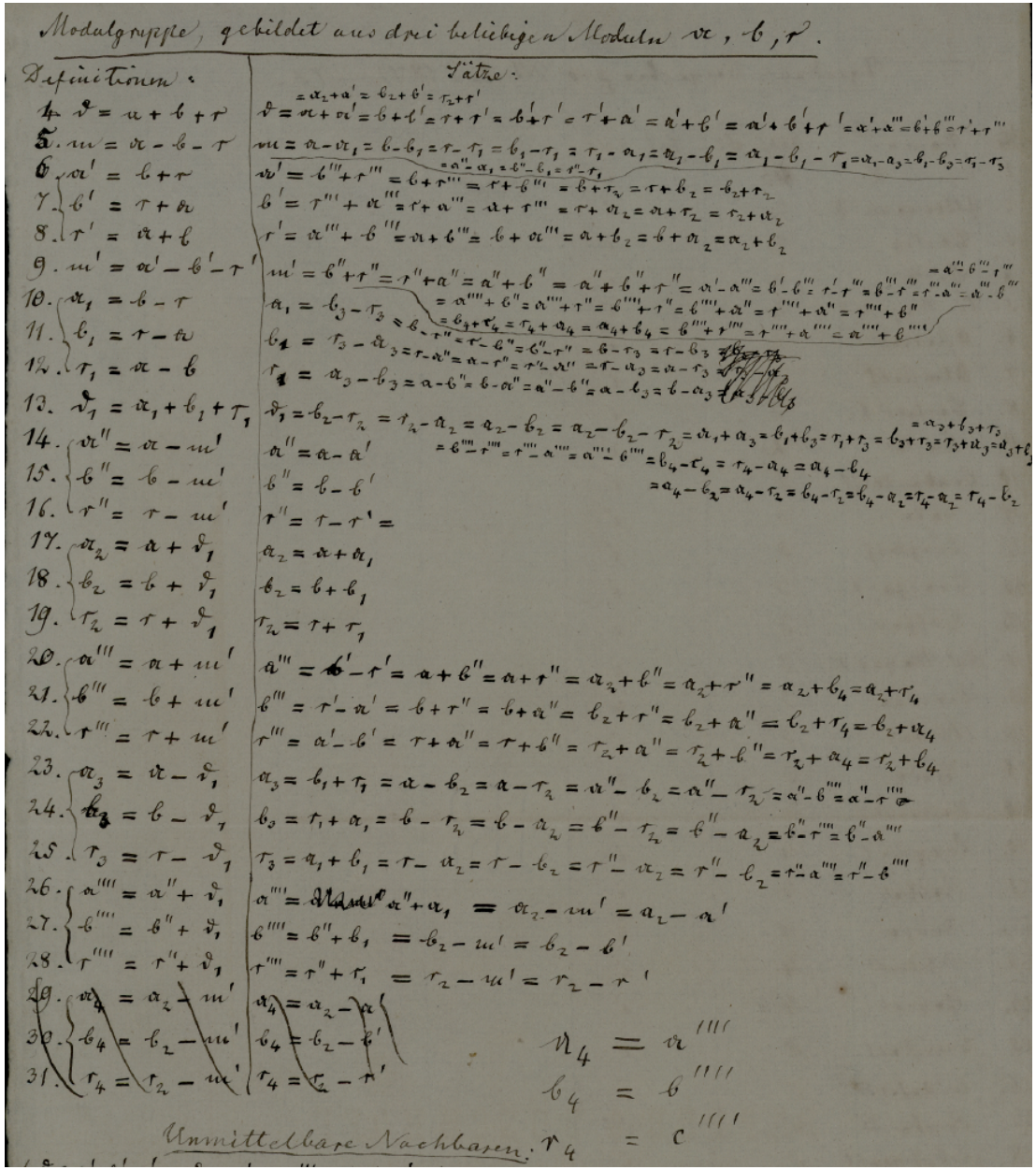


Figure: Cod. Ms. Dedekind X 11-1, p. 27v.

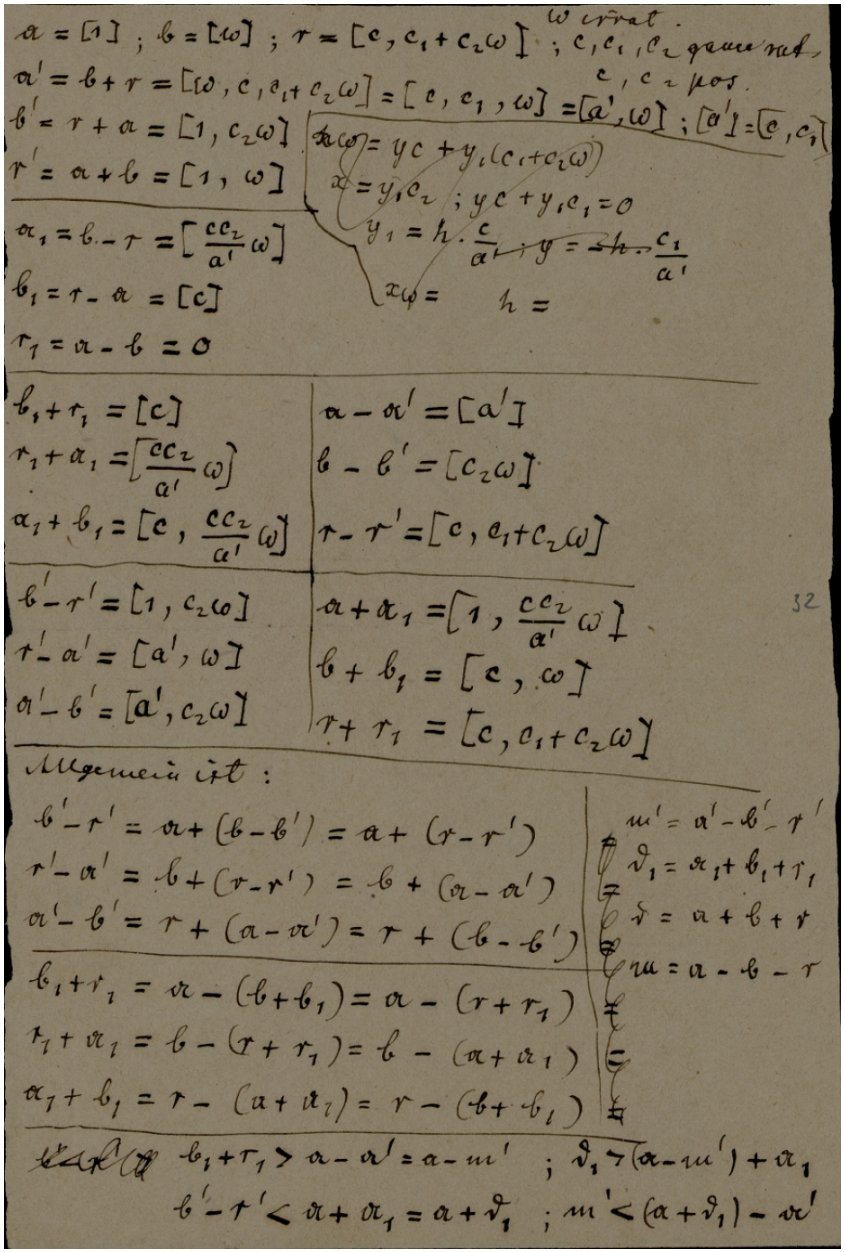


Figure: Cod. Ms. Dedekind X 11-1, p.32r.

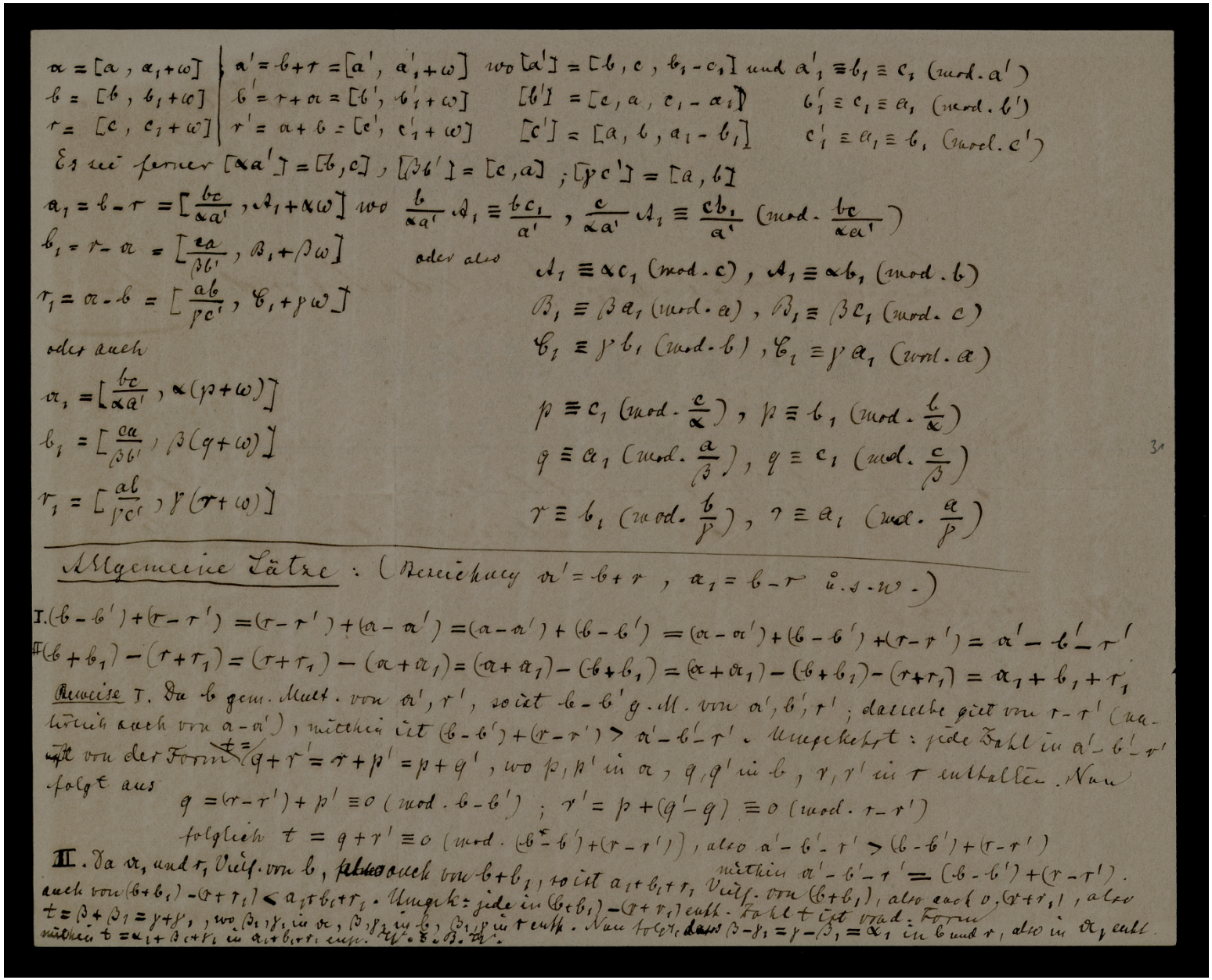


Figure: Cod. Ms. Dedekind X 11-1, p. 31r.

L'ordre

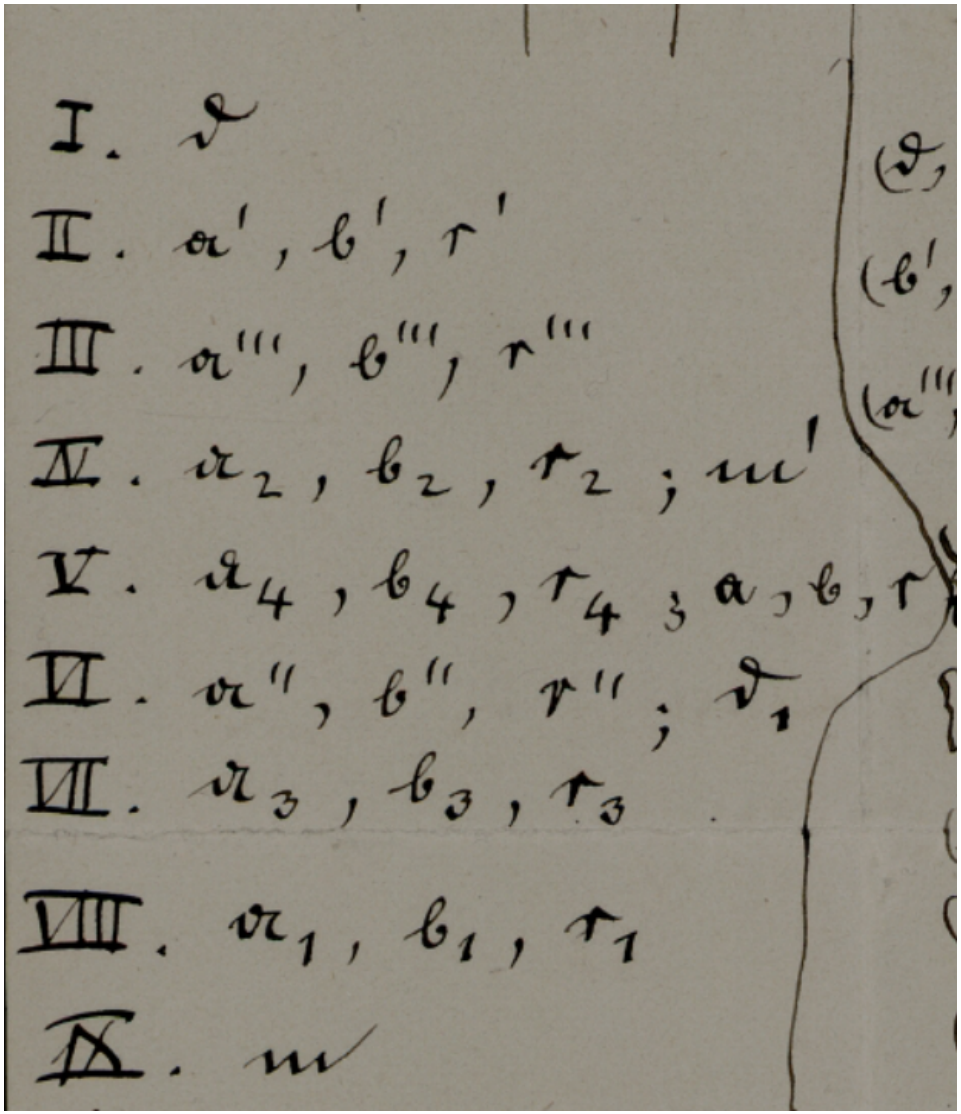


Figure: Cod. Ms. Dedekind X 11-1, p.24v.

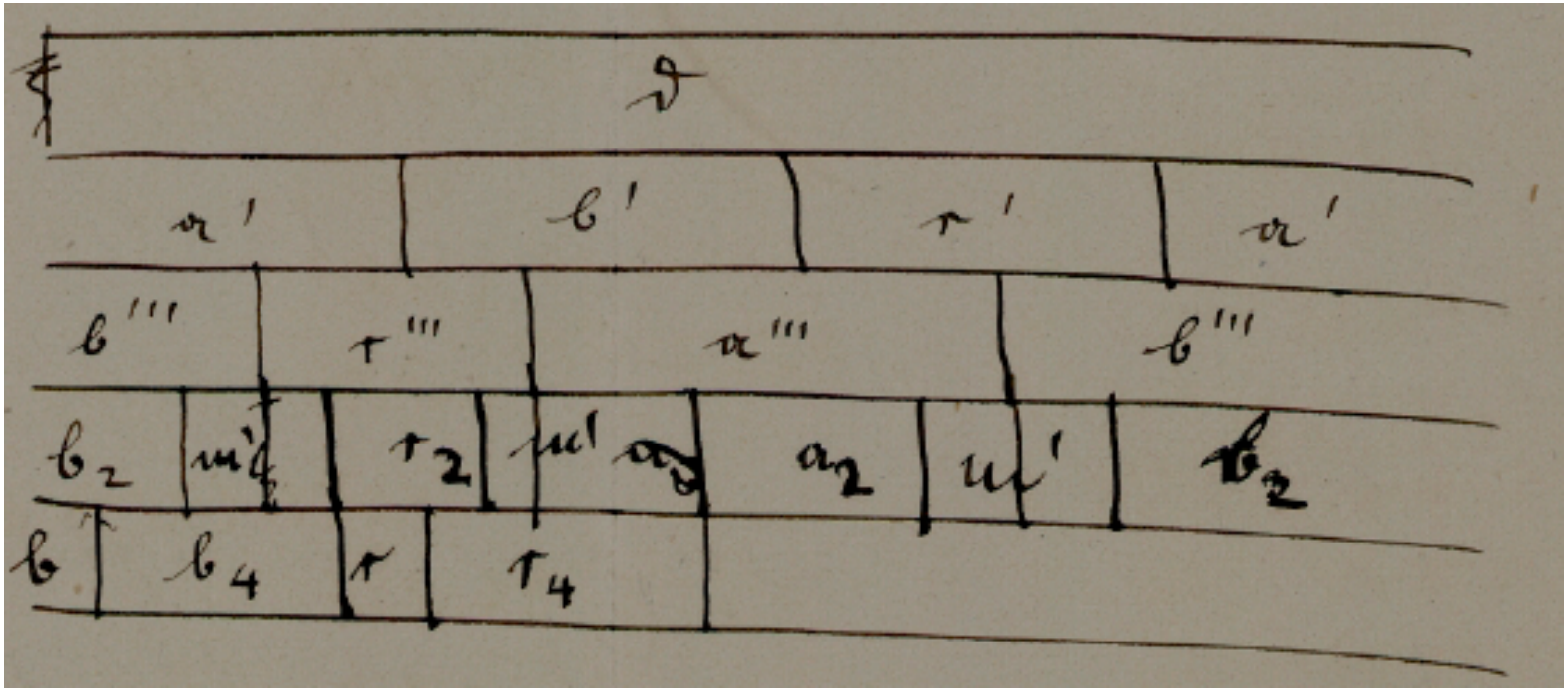


Figure: Cod. Ms. Dedekind X 11-1, p.24v.

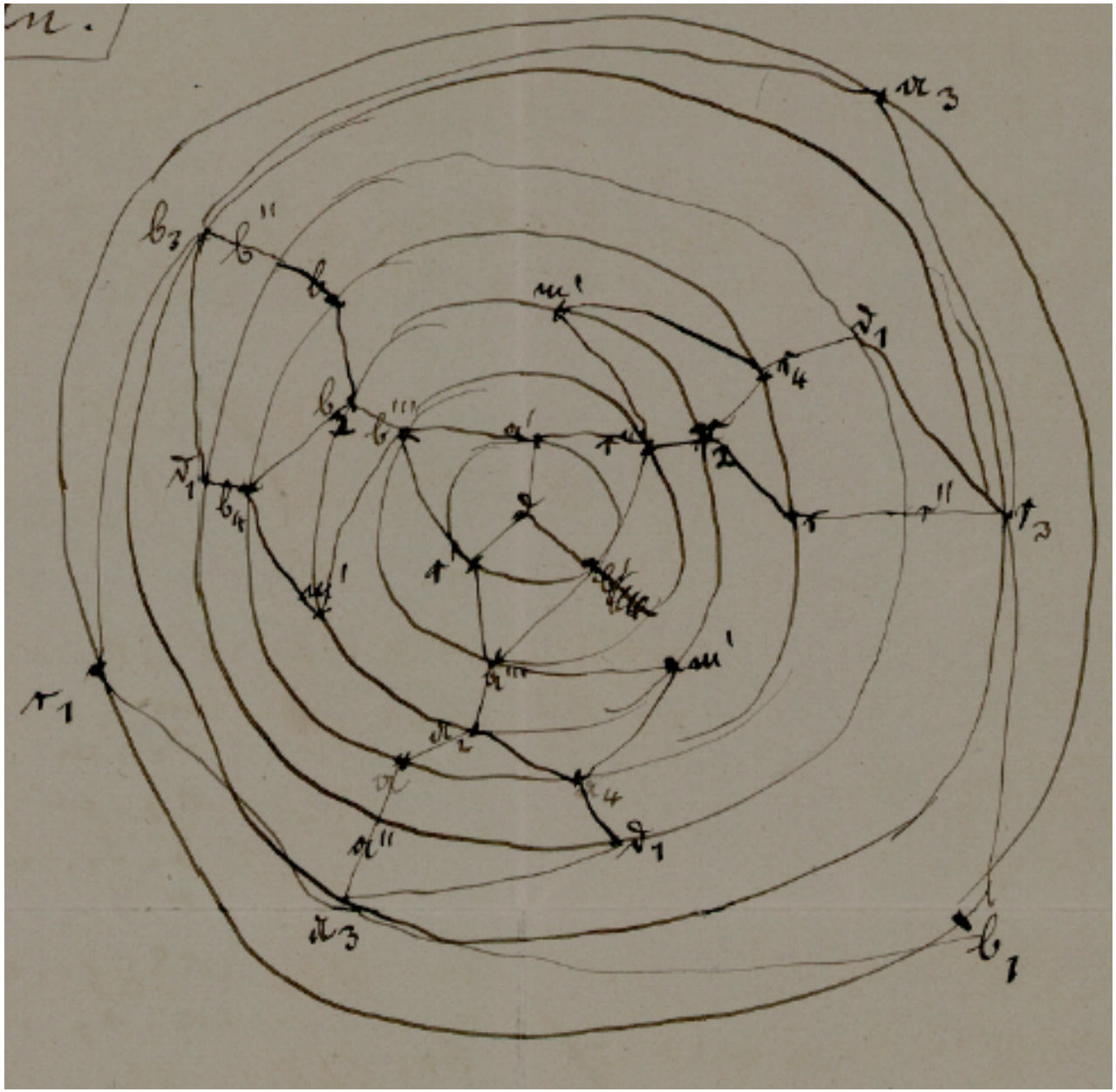


Figure: Cod. Ms. Dedekind X 11-1, p.24v.

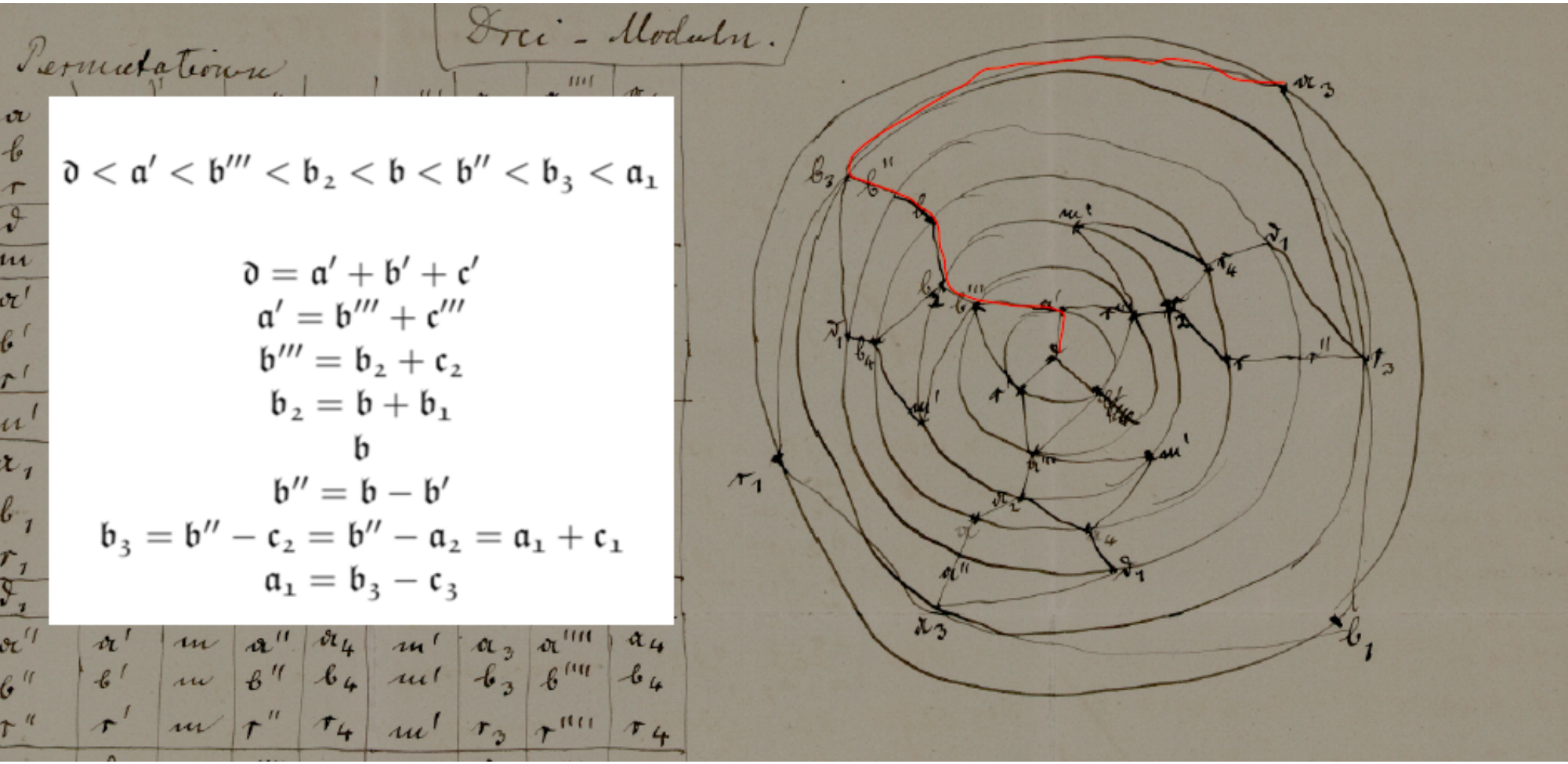


Figure: Cod. Ms. Dedekind X 11-1, p.24v.

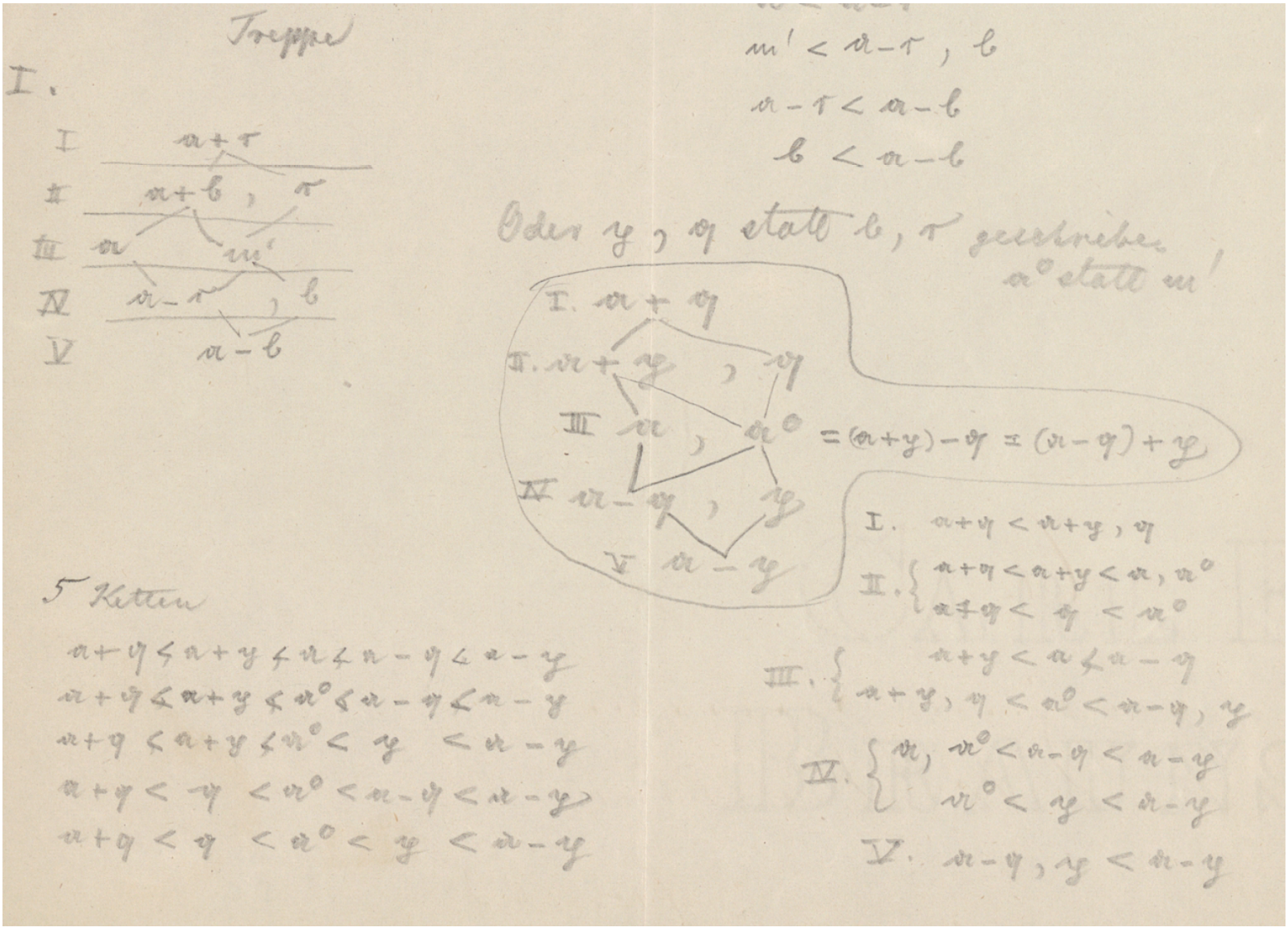
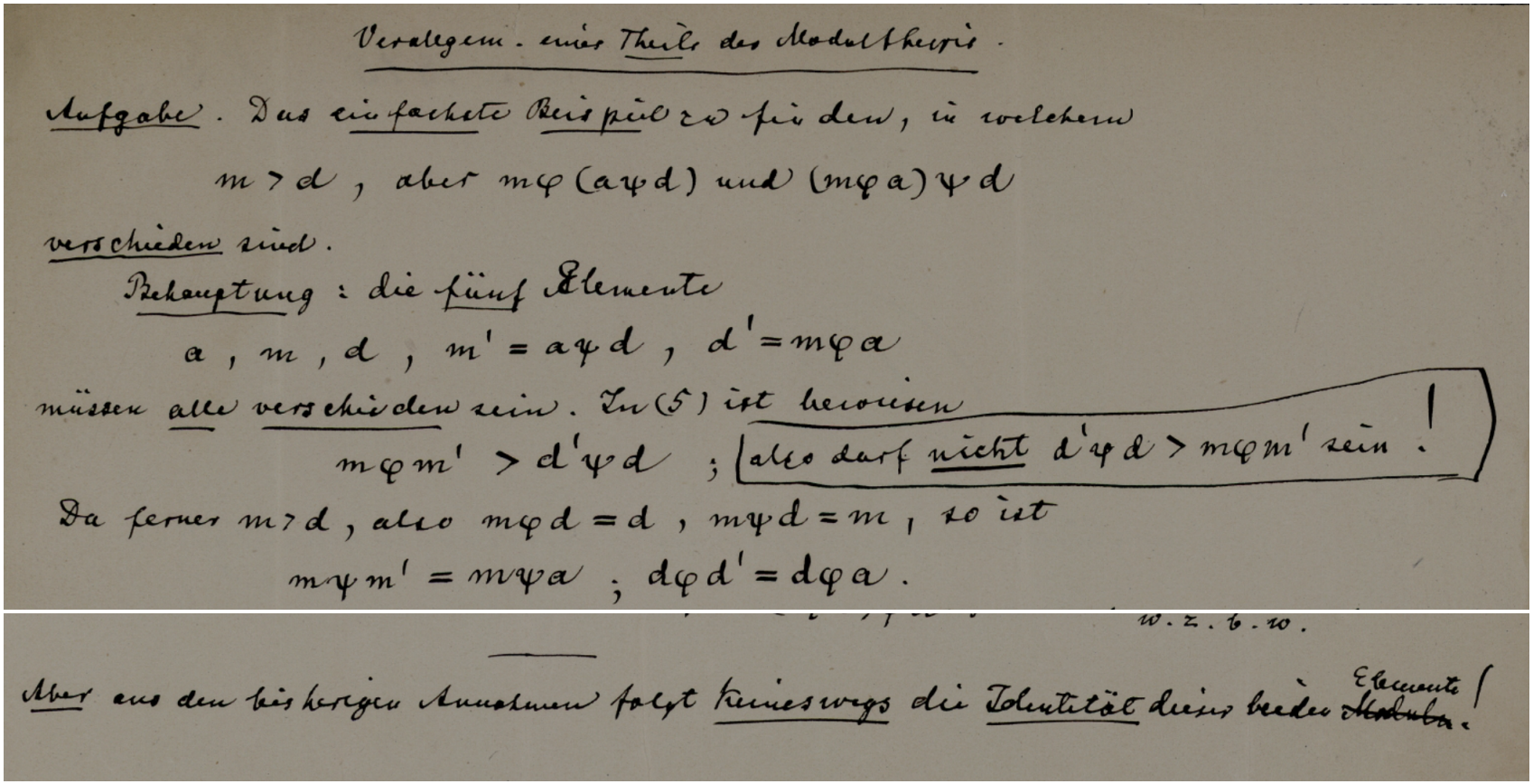


Figure: Cod. Ms. Dedekind X 10, p. 9r.

Vers la généralisation ?

Deux aspects des recherches :

- Penser aux ensembles générés par les opérations entre modules comme étant des "groupes".
  - Ensembles (en général, finis, dans les cas qu'étudie Dedekind) fermés par $+$ et $-$.
  - Beaucoup d'études de cas.
- Penser aux opérations comme pouvant s'appliquer à d'autres opérandes.
  - Modules comme objets plutôt qu'ensembles de nombres : calculer avec les modules comme on calcule avec des nombres.
  - Opérations comme indépendantes des opérandes.
  - Études de cas en 'remplaçant' les modules par des idéaux, groupes, jusqu'à considérer seulement des "éléments" indéterminés.



Veralgem. eines Theils der Modultheorie.

Aufgabe. Das einfachste Beispiel zu finden, in welchem

$m > d$, aber $m\varphi(a\psi d)$ und $(m\varphi a)\psi d$

verschieden sind.

Behauptung: die fünf Elemente

$a, m, d, m' = a\psi d, d' = m\varphi a$

müssen alle verschieden sein. In (5) ist bewiesen

$m\varphi m' > d'\psi d$; also darf nicht $d'\psi d > m\varphi m'$ sein!

Da ferner $m > d$, also $m\varphi d = d$, $m\psi d = m$, so ist

$m\psi m' = m\psi a$; $d\varphi d' = d\varphi a$.

w. z. b. w.

Aber aus den bisherigen Annahmen folgt keineswegs die Identität dieser beiden Elemente!

Figure: Cod. Ms. Dedekind X 10, p. 9r.

"Sur le dualisme dans la théorie des modules"

Dans un système fini ou infini S d'éléments $a, b, c, \ldots$ dont la signification est laissée complètement indéterminée, on prend deux sortes de combinaisons φ et ψ, qui à partir de deux éléments distincts ou identiques a, b produisent toujours deux éléments complètements déterminés du même système S désignés par $a\varphi b, a\psi b$. Elles obéissent les six lois suivantes

$$
\begin{array}{cc}
\cancel{a\varphi a = a} & \cancel{(1)} \\
a\varphi b = b\varphi a & \cancel{(2)}\,(1) \\
(a\varphi b)\varphi c = a\varphi(b\varphi c) & \cancel{(3)}\,(2) \\
\cancel{a\psi a = a} & \cancel{(1')} \\
a\psi b = b\psi a & \cancel{(2')}\,(1') \\
(a\psi b)\psi c = a\psi(b\psi c) & \cancel{(3')}\,(2') \\
a\psi(a\varphi b)\,\cancel{(a\varphi b)\psi a} = a & \cancel{(4)}\,(3) \\
a\varphi(a\psi b)\,\cancel{(a\psi b)\varphi a} = a & \cancel{(4')}\,(3').
\end{array}
$$

(Cod. Ms. Dedekind XI 1, p. 1r-2r)

Modulgruppen

> *Un système M de modules est appelé un groupe lorsque les modules* $\mathfrak{a}+\mathfrak{b}, \mathfrak{a}-\mathfrak{b}$ *formés par n'importe quels deux modules* $\mathfrak{a}, \mathfrak{b}$ *appartiennent au même système.*

(Cod. Ms. Dedekind XI 1, 29r.)

“Théorie (logique) plus générale”

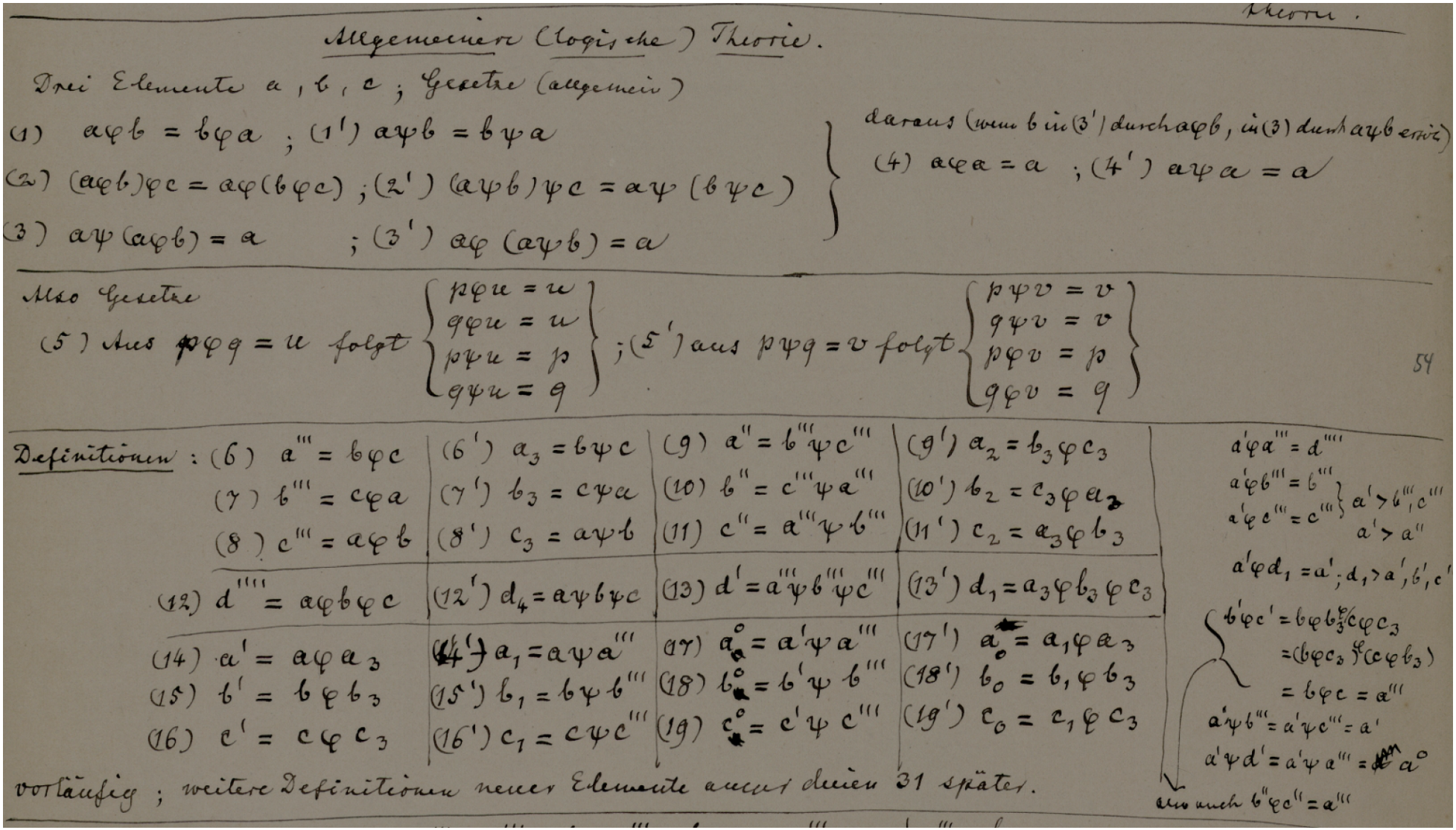


Figure: Cod. Ms. Dedekind X 11-2, p. 54r.

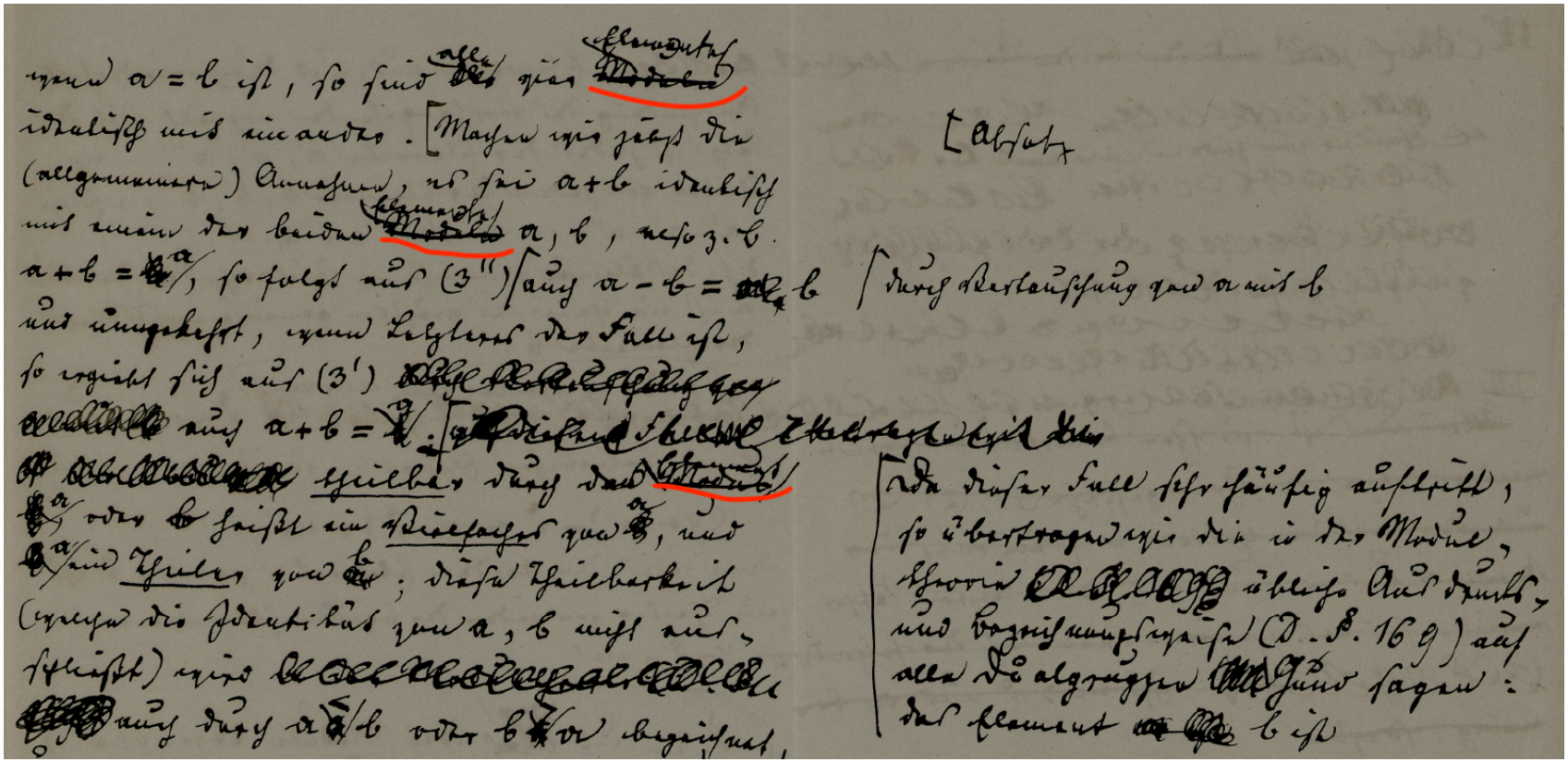


Figure: Cod. Ms. Dedekind X 11-2, p. 19r.

Conclusion

Répondant à des critiques de Kronecker sur sa théorie des idéaux en 1882, Dedekind écrit :

> *Il est de plus dit que je "mets le concept de tous les nombres divisibles par un diviseur idéal au cœur de ce développement" (. . .). Il peut sembler que j'ai défini un "idéal" à partir des "nombres idéaux" de Kummer, alors que j'ai plutôt donné la priorité à la définition complètement indépendante et invariante par les deux propriétés [de clôture] (Dirichlet [Vorlesungen über Zahlentheorie] §163 de la seconde [édition], §167-168 de la troisième, et aussi §§11, 19 dans "Sur la théorie des nombres entiers algébriques"). Peut-être la remarque de Kronecker est-elle due à la présentation historique de la chaîne de pensées qui m'a mené à l'introduction du concept d'idéal (introduction de "Sur la théorie des nombres entiers algébriques", p. 8-10)!*

(H. Edwards, O. Neumann, et W. Purkert, 1982, Dedekind's 'Bunte Bemerkungen' zu Kroneckers 'Grundzüge'. *Archive for History of Exact Sciences*, 27(1):49–85, 63)