Computability in Algebraic Number Theory: Hensel to Zassenhaus

Steve Kieffer
Simon Fraser University
12 April 2012

Objects associated with number fields:

- integral basis
- for each rational prime p, its ideal factors
- discriminant
- group of fundamental units
- class number
- class group
- Galois group

Are they computable?

A philosophical divide

"The definition of irreducibility given in Art. 1 lacks a firm foundation until a method is given that makes it possible to determine whether a given example does or does not satisfy it."
— Kronecker, *Grundzüge* §4, 1882

"I prove now the fundamental theorem for the whole theory: A polynomial $F(x)$ with p-adic coefficients decomposes uniquely into irreducible p-adic factors, and there is a finite procedure to compute these factors to any desired degree of accuracy."
— Hensel, *Th. Alg. Zahl.*, 1908

"Even if there were such a theory, based on calculation, it still would not be of the highest degree of perfection, in my opinion. It is preferable ... to seek proofs based immediately on fundamental characteristics, rather than on calculation..."
— Dedekind, *STNEA*, 1877

"On the basis of his way of looking at things, Kronecker forbids already the simplest irrational number $\sqrt{2}$; he introduces the concept of the modulus $x^2 - 2$ in place of this 'inadmissible' concept. ..."
— Hilbert, Göttingen, Summer 1920

The integral basis

In Dedekind:

- slick existence proof, using well-ordering principle
- Paraphrasing: "Since the discriminants of all these modules $\mathfrak{a}, \mathfrak{b}, \ldots$ are nonzero integers, there must be such a module $\mathfrak{a}$ whose discriminant is least in absolute value, and then by the previous theorem $\mathfrak{a} = \mathcal{O}_F$. Therefore $\mathcal{O}_F$ has a basis." (D-D 4 ed. p. 538)

In Hensel:

1. Compute the discriminant d of $\mathbb{Q}(\alpha)$.
2. Consider every number of the form

$$\frac{v_0 + v_1\alpha + \cdots + v_{n-1}\alpha^{n-1}}{d}$$

   with all $0 \leq v_i < d$. (There are only finitely many.) For each one, check whether it is an integer or not, in the following way....
3. From the integers just found, select an integral basis in the following way.... (TAZ pp. 112-115)

Unique factorization into prime ideals

In Dedekind:

- slick proof, using ascending chain condition, and fact that any ideal $\mathfrak{a} \neq \mathcal{O}_F$ is divisible by at least one prime ideal (D-D 4 ed. pp. 561-562)

In Hensel:

1. Compute min. poly. of $\beta \in \mathbb{Q}(\alpha)$, and compute all the rational primes $p_1, \ldots, p_r$ dividing its constant term.
2. For each p_i:
   (a) Factor min. poly. of α over $\mathbb{Q}_{p_i}$ into irreducible f_j.
   (b) Compute prime number π_{ij} in extension of $\mathbb{Q}_{p_i}$ for each factor f_j.
   (c) Compute π_{ij}-adic order e_{ij} of const. term in corresp. factor of min. poly. of β over $\mathbb{Q}_{p_i}$.
3. Output: $\beta \sim \prod \mathfrak{p}_{ij}^{e_{ij}}$. (TAZ Ch. 7 § 4)

Unique factorization into prime ideals

In Dedekind:

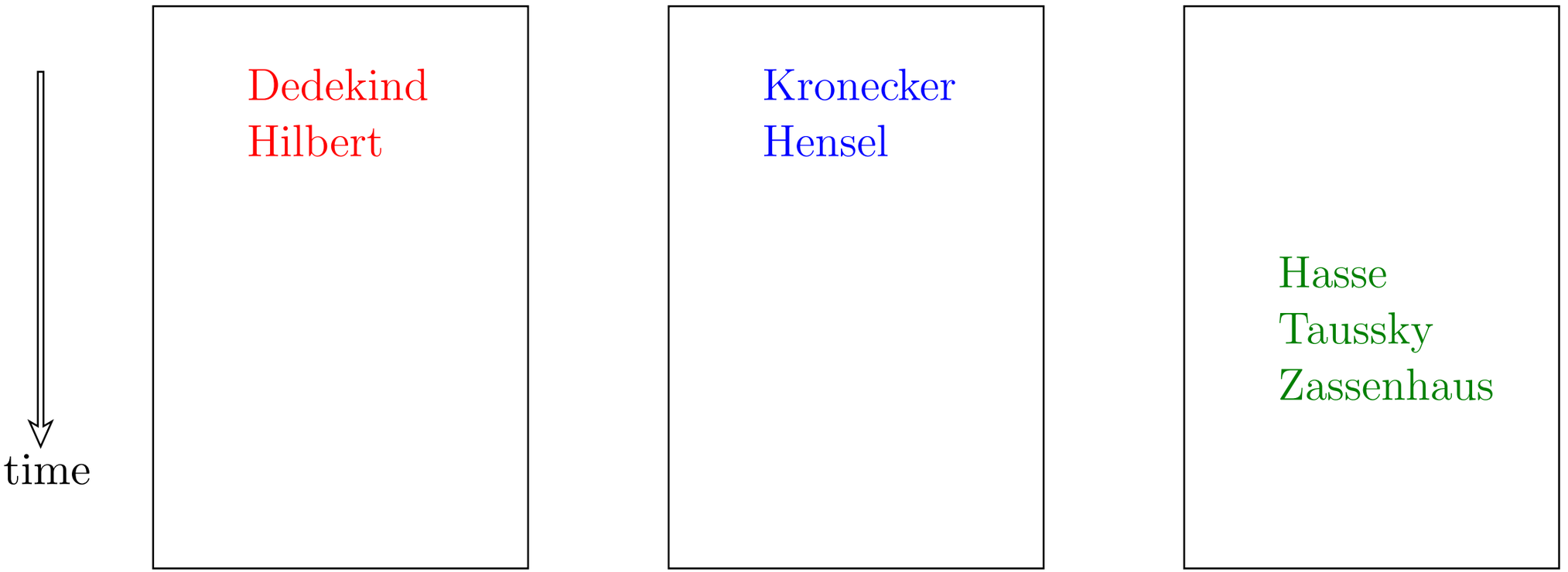
- slick proof, using ascending chain condition, and fact that any ideal $\mathfrak{a} \neq \mathcal{O}_F$ is divisible by at least one prime ideal (D-D 4 ed. pp. 561-562)

In Hensel:

1. Compute min. poly. of $\beta \in \mathbb{Q}(\alpha)$, and compute all the rational primes $p_1, \ldots, p_r$ dividing its constant term.
2. For each p_i:
   (a) Factor min. poly. of α over $\mathbb{Q}_{p_i}$ into irreducible f_j.
   (b) Compute prime number π_{ij} in extension of $\mathbb{Q}_{p_i}$ for each factor f_j.
   (c) Compute π_{ij}-adic order e_{ij} of const. term in corresp. factor of min. poly. of β over $\mathbb{Q}_{p_i}$.
3. Output: $\beta \sim \prod \mathfrak{p}_{ij}^{e_{ij}}$. (TAZ Ch. 7 § 4)

Styles of number theory

and a few representatives



Existence

Computability in principle ("constructivity")

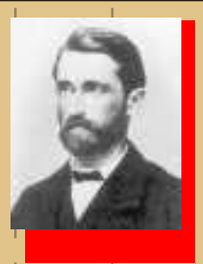
Computability in practice

Kummer (1810-1893)

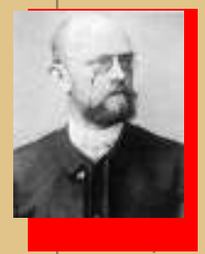
Kronecker (1823-1891)

Dedekind (1831-1916)

Hensel (1861-1941)



Hilbert (1862-1943)



Weyl (1885-1955)

Hasse (1898-1979)

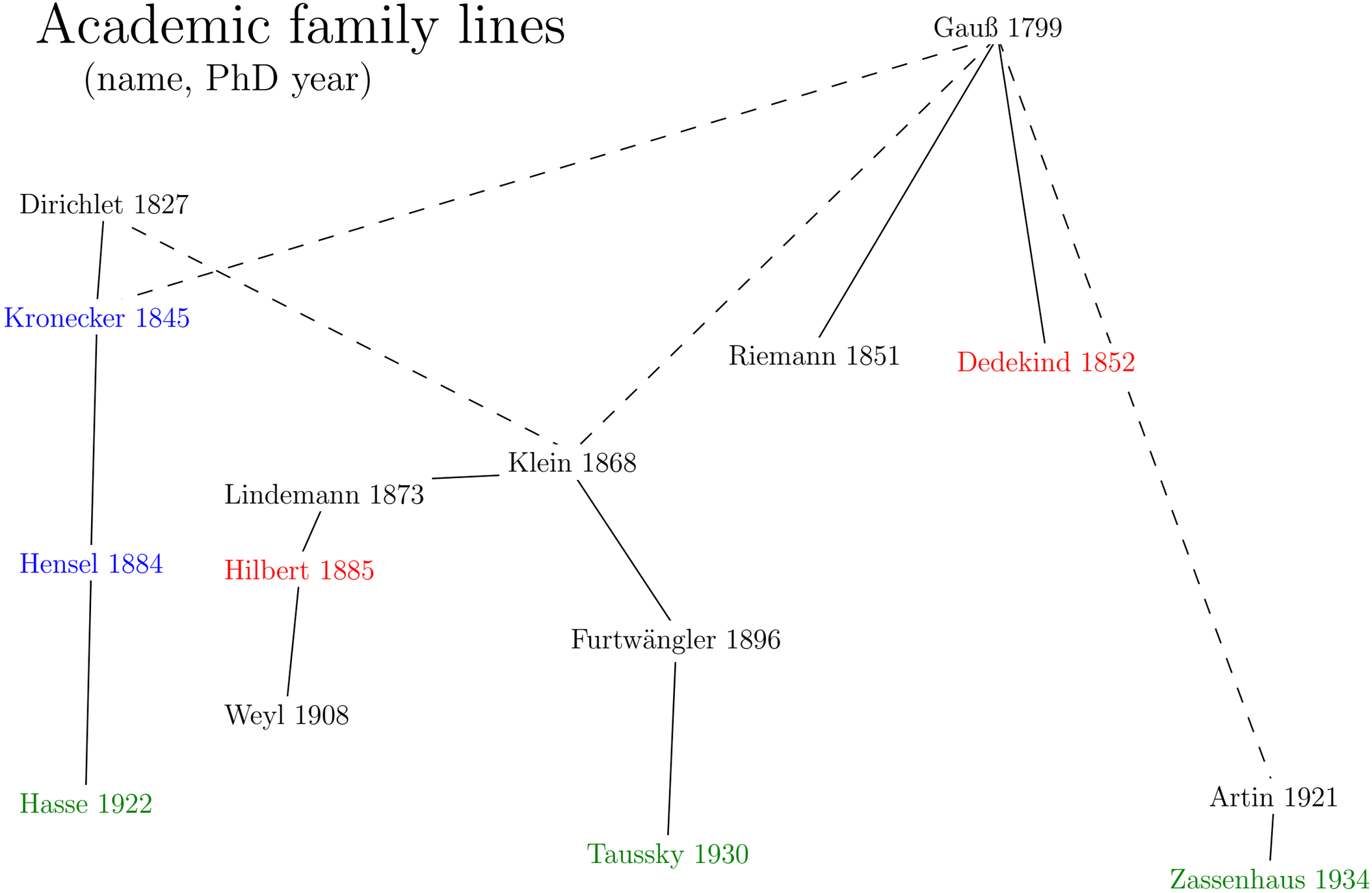
Taussky (1906-1995)

Zassenhaus (1912-1991)

1800 1850 1900 1950 2000

Academic family lines

(name, PhD year)



My questions:

- How did we get from Hensel to Zassenhaus?
  - Hensel used "Hensel's lemma" in 1904 to factor polynomials over $\mathbb{Q}_p$, in principle.
  - Zassenhaus used it in 1968 to factor polynomials over $\mathbb{Z}$ in practice.
- Was interest in computability passed on from Hensel to Zassenhaus?

My questions:

- How did we get from Hensel to Zassenhaus?
  - Hensel used "Hensel's lemma" in 1904 to factor polynomials over $\mathbb{Q}_p$, in principle.
  - Zassenhaus used it in 1968 to factor polynomials over $\mathbb{Z}$ in practice.
- Was interest in computability passed on from Hensel to Zassenhaus?

Basic finding:

Chain of influence: Hensel $\rightarrow$ Hasse $\rightarrow$ Taussky $\rightarrow$ Zassenhaus

Hasse → Taussky

- T's PhD 1930, Vienna, Furtwängler, CFT
- 1934: computing with A. Scholz (1904-1942), tables of Hasse
- 1936 letter to Hasse re computing class numbers
- war work, computers, NBS, SEAC & SWAC 1950
- early 1950s correspondence
  - evidence for FLT
  - class numbers
  - books from Hasse: Weyl, KAZ
  - 1953 survey

Taussky-Scholz 1934

1) $\vartheta \equiv 5, 6, -11$ (313) $\vartheta \equiv 19, 57, -76$ $\langle 2\rangle = \langle 11\rangle = \langle 13\rangle = \langle 17\rangle = \varrho.$

$\varepsilon \equiv -3, -4, 13$ $\varepsilon \equiv -17, -55, 78$ $\langle 3\rangle = \langle 29\rangle = \varrho^2.$

$\langle\varepsilon\rangle = \varrho, 1, \varrho^2$ $\langle\varepsilon\rangle = \varrho, \varrho, \varrho$ $\langle 5\rangle = \langle 7\rangle = \langle 19\rangle = 1.$

Nach dem zulässigen Modul $q = 313$ gilt dann:

$$\mathfrak{j}_{27}^2 \equiv 128 \pm 12; \quad \chi = \varrho^2, \varrho.$$
$$\mathfrak{j}_{23}^3 \equiv -50 \pm 6; \quad \chi = 1.$$

Es wird also $\mathfrak{j}_{23}$ Hauptideal in K_{11}, nicht $\mathfrak{j}_{27}$.

[3] $F(x) = x^3 - 16x - 27 = 0.$

δ	$\lvert N(\delta)\rvert$	Zerfällung
ϑ	27	$\bar{3}_1^3$
$\vartheta - 4$	27	$\bar{3}_2^3$
$\vartheta + 4$	27	$\bar{3}_3^3$
$\vartheta + 2$	3	$\bar{3}_2$

Also $\varepsilon = \dfrac{\vartheta - 4}{(\vartheta + 2)^3}; \quad \sigma = \vartheta - 4.$

(9) $\vartheta \equiv 0, 4, -4$ (277) $\vartheta \equiv 14, 47, -61$ $\langle 2\rangle = \langle 13\rangle = 1;\ \langle 3\rangle = \varrho;$

$\sigma \equiv -4, 0, 1$ $\sigma \equiv 10, 43, -65$ $\langle 5\rangle = \langle 7\rangle = \varrho^2.$

$\langle\varepsilon\rangle = \varrho^2, \varrho, 1$ $\langle\sigma\rangle = \varrho^2, \varrho^2, \varrho^2$

Wir können $q = 277$ setzen; es ist dann

$$\mathfrak{j}_{11}^3 = \frac{45 + \sqrt{D}}{2} \equiv 25, 20; \quad \chi = \varrho, \varrho^2.$$
$$\mathfrak{j}_{23}^3 = \frac{213 + \sqrt{D}}{2} \equiv -168, 104; \quad \chi = 1.$$

Taussky-Scholz 1934

"These studies do not require the Artin Reciprocity Law. *It will be decided by means of relations in the field of rational numbers*, which classes become principal in the unramified relative-cubic extension field. For this section the theorems of Hasse on cubic fields (Math. Zeitschrift 31) were essential."

Taussky → Zassenhaus

- Z's PhD 1934, Hamburg, Artin, Gp. Th.
- first purely NT paper: 1949
- 1959: visit to Caltech, work with Taussky

> "Zassenhaus's tendency to computational algebraic number theory came out for the first time at Caltech during his visit 1959."

Caltech 1959

- a computational equivalent of an element λ;
- a computational equivalent of an ideal $\mathfrak{a}$;
- a way to decide "=" on elements;
- a way to decide "=" on ideals;
- a way to compute the product of two elements;
- a way to compute the product of two ideals;
- a way to compute the quotient of two ideals;

Zassenhaus

- After 1959: four goals:
  - Galois group
  - integral basis
  - unit group
  - class group
- 1965: ORDMAX, 1971: "Round II"
- 1968: p-adic methods
  - solve CFT problem set by Hasse
  - factor poly. over $\mathbb{Z}$ using Hensel's lemma

Epilogue

- 1969 Oxford conference
- 1972 survey by H. Zimmer
- Pohst-Zassenhaus 1989
- H. Cohen 1993, 2000