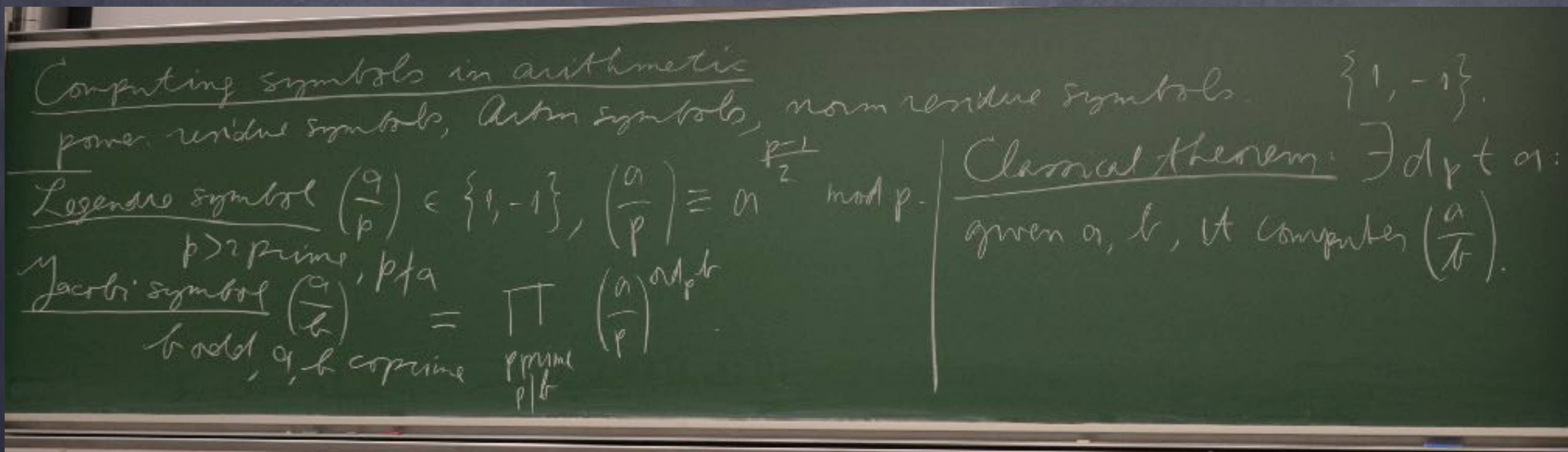
# Computing symbols in arithmetic

Hendrik Lenstra

NutMiC 2019

Paris




Note: dpta = deterministic polynomial time algorithm

## Computing symbols in arithmetic

power residue symbols, Artin symbols, norm residue symbols $\{1,-1\}$.

**Legendre symbol** $\left(\frac{a}{p}\right) \in \{1,-1\}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

$p>2$ prime, $p \nmid a$

Jacobi symbol $\left(\frac{a}{\cdot}\right)$ : $\prod \left(\frac{a}{\cdot}\right)^{\mathrm{ord}_p b}$

**Classical theorem**: $\exists$ alg $t$ a: given $a, b$, it computes $\left(\frac{a}{b}\right)$.

**Reciprocity laws.** Let $a, b \in \mathbb{Z}$, odd & coprime, $\boxed{b>0}$ then

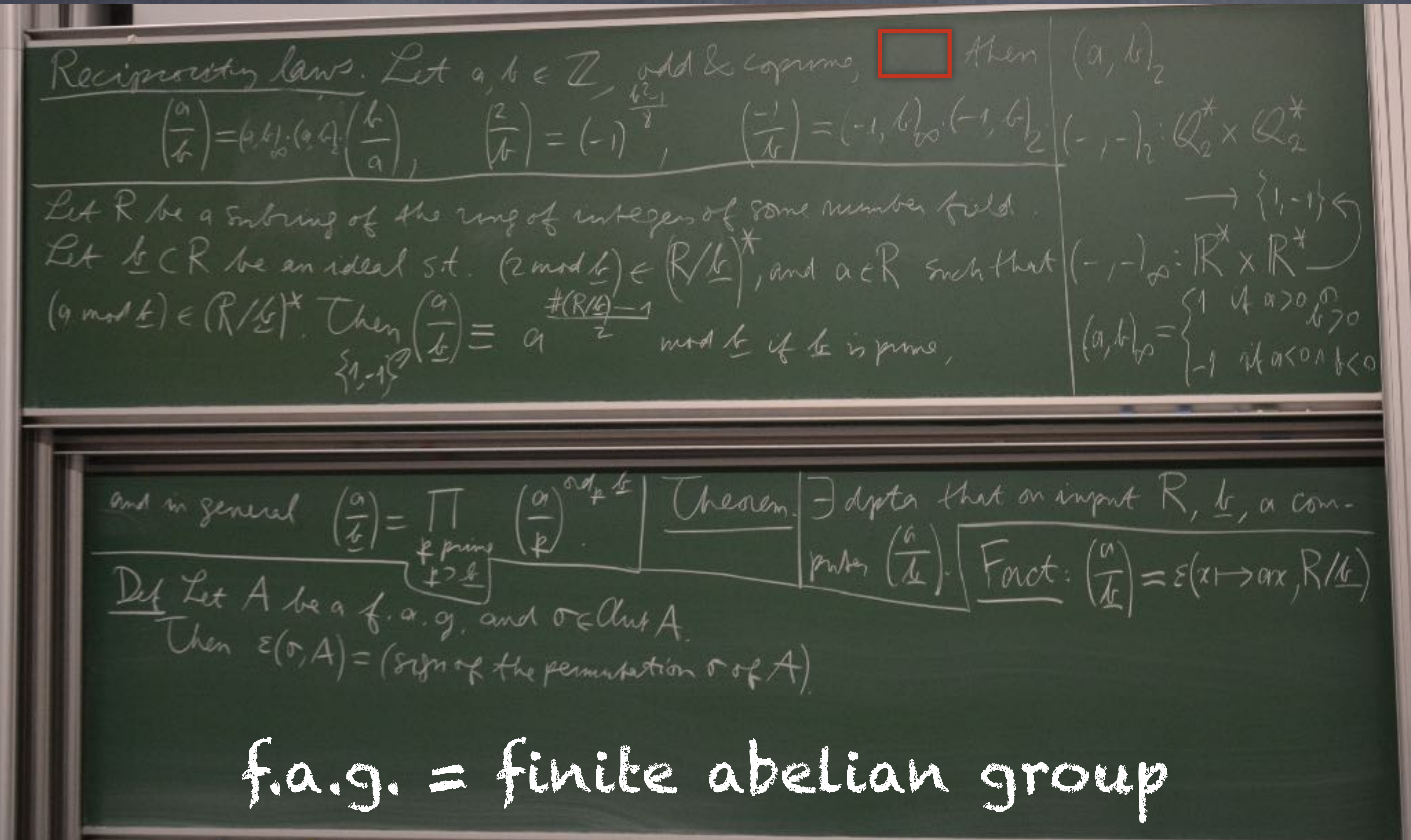
$$\left(\frac{a}{b}\right) = \underbrace{(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}}_{(a,b)_2}\left(\frac{b}{a}\right), \quad \left(\frac{2}{b}\right) = \underbrace{(-1)^{\frac{b^2-1}{8}}}_{(2,b)_2}, \quad \left(\frac{-1}{b}\right) = \underbrace{(-1)^{\frac{b-1}{2}}}_{(-1,b)_2}.$$

$(a,b)_2$

$(-,-)_2 : \mathbb{Q}_2^* \times \mathbb{Q}_2^* \longrightarrow \{1,-1\}$

$(-,-)_\infty : \mathbb{R}^* \times \mathbb{R}^* \longrightarrow \{1,-1\}$

$$(a,b)_\infty = \begin{cases} 1 & \text{if } a>0 \text{ or } b>0 \\ -1 & \text{if } a<0 \text{ and } b<0 \end{cases}$$




f.a.g. = finite abelian group

... in general $\left(\frac{a}{b}\right) = \prod_{\substack{p \text{ prime} \\ p \mid b}} \left(\frac{a}{p}\right)$.

**Theorem:** ... computes $\left(\frac{a}{b}\right)$.

**Fact:** $\left(\frac{a}{b}\right) = \varepsilon(x \mapsto ax, R/b)$

**Def** Let $A$ be a f.a.g. and $\sigma \in \operatorname{Aut} A$.
Then $\varepsilon(\sigma, A) = $ (sign of the permutation $\sigma$ of $A$).

**Lemma** If $B < A$ is a subgp with $\sigma B = B$, then
$$\varepsilon(\sigma, A) = \varepsilon(\sigma|_B, B) \cdot \varepsilon(\bar{\sigma}, A/B)$$

**Theorem** Restrict to $\# A$ odd. $\exists$ algo that given $A, \sigma$ computes $\varepsilon(\sigma, A)$.

**Lemma** If $A \cong (\mathbb{Z}/b\mathbb{Z})^{\oplus r}$ for some odd $b \in \mathbb{Z}$, $r \in \mathbb{Z}_{\geq 0}$, then $\varepsilon(\sigma, A) = \left(\frac{\det \sigma}{b}\right)$.

$A = (\mathbb{Z}/n_1\mathbb{Z}) \oplus \dots \oplus (\mathbb{Z}/n_t\mathbb{Z})$, $1 < n_1 \mid n_2 \mid \dots \mid n_t$

$A/n_1 A \cong (\mathbb{Z}/n_1\mathbb{Z})^{\oplus t}$

Let $F$ be a <u>local field</u>, i.e. a finite extension of $\mathbb{Q}_p$ for some $p$ prime or $\infty$ ($\mathbb{Q}_\infty = \mathbb{R}$).

$$(-,-)_F : F^* \times F^* \to \{1,-1\}, \quad (a,b)_F = \begin{cases} 1 & \text{if } \exists\, x,y \in F : ax^2 + by^2 = 1 \\ -1 & \text{otherwise} \end{cases}$$

$$\left.\begin{array}{l} (a,b) = (b,a)^{-1} \\ (aa',b) = (a,b)\cdot(a',b) \\ (a,1-a) = 1 \quad (a \neq 1) \end{array}\right\} (a,-a) = 1$$

<u>$p \neq 2$</u>: $(a,b)_{\mathbb{Q}_p} = \left(\frac{c}{p}\right)$, for

$$c = (-1)^{(\mathrm{ord}_p a)(\mathrm{ord}_p b)} \cdot \frac{b^{\mathrm{ord}_p a}}{a^{\mathrm{ord}_p b}}$$

<u>$p = 2$</u>: $a = 2^{a_2} \cdot (-1)^{a_{-1}} \cdot 5^{a_5} \cdot \alpha^2$, with $a_2, a_{-1}, a_5 \in \{0,1\}$, $\alpha \in \mathbb{Q}_2^*$.

$b$ likewise

then

$$(a,b)_{\mathbb{Q}_2} = (-1)^{a_{-1}b_{-1} + a_2 b_5 + a_5 b_2}$$

Theorem. ∃ algo that on input $F$, $a$, $b$, computes $(a,b)_F$

Jan Bouw. $F \xrightarrow{\mathrm{ord}=\mathrm{ord}_F} \mathbb{Z}\cup\{\infty\}$, $\mathrm{ord}\,0=\infty$, $F^* \xrightarrow{\mathrm{ord}} \mathbb{Z}$, $\mathcal{O}=\{x : \mathrm{ord}\,x \geq 0\}$ ring o

$F \supset \mathbb{Q}_p$, $p$ prime | $\pi \in F$ is called prime if $\mathrm{ord}\,\pi = 1$. Field $\mathcal{O}/\pi\mathcal{O} = \mathbb{F}_q$, $q$ = powe

$p=2$.

$$F^* \supset \underbrace{\mathcal{O}^*}_{\mathbb{Z}} \supset \underbrace{1+\pi\mathcal{O}}_{\mathbb{F}_q^*} \supset \underbrace{1+\pi^2\mathcal{O}}_{\cong \mathbb{F}_q^+} \supset \underbrace{\dots}_{\cong \mathbb{F}_q^+}$$

$F^* = \pi^{\mathbb{Z}} \times \mathcal{O}^*$, $\mathcal{O}^* = \langle \zeta_{q-1} \rangle \times (1+\pi\mathcal{O})$

Fact: $F^* = H_\pi \sqcup (H_\pi \delta)$

Let $\pi$ be a prime element. Elements $b$ with $(\pi, b) = 1$:

- $b = -\pi$
- $b = c^2$ $(c \in F^{*})$
- $b \in \langle \zeta_{q-1} \rangle$
- $b = 1 - \zeta \pi^i$, $\zeta \in \langle \zeta_{q-1} \rangle$, $i \in \mathbb{Z}$ odd.

$(\pi^i, 1-\zeta\pi^i) = 1$

$H_\pi = $ (subgroup of $F^*$ generated by the $b$'s on the left)

$(a,b) = (b,a)^{-1}$

$(aa', b) = (a,b)\cdot(a',b)$

$(a, 1-a) = 1 \quad (a \neq 1)$

$\Rightarrow (a,-a) = 1$

A distinguished unit is an element $\delta \in (1+4\mathcal{O}) \setminus F^{*2}$, $\boxed{(\pi,\delta) = -1}$

# Author's Notes

The algorithm that I explained for computing the Jacobi symbols in algebraic number fields was taken from a paper "Computing Jacobi symbols in algebraic number fields", Nieuw Arch. Wisk. 13 (1995), 421-426 of mine. Much basic information about power residue symbols and the norm residue symbol can be found in the exercises at the end of the Brighton proceedings volume "Algebraic number theory" edited by Cassels and Fro:hlich (Academic Press, 1967), which I found myself more useful than the book "Class field theory" by Artin and Tate. The paper "Calculating the power residue symbols and Ibeta" by Koen de Boer and Carlo Pagano (ISSAC'17, July 25-28, 2017, Kaiserslautern, Germany) contains a promising approach to computing general power residue symbols; it is my understanding that Koen de Boer is working on a sequel to this paper, in which Artin symbols will also be considered. The algorithm for computing the norm residue symbol that I outlined in my lecture will be included in the Leiden PhD thesis of Jan Bouw, which will hopefully be available within a year or so. It is strongly inspired by the appendix "Continuous Steinberg symbols" to John Milnor's "Introduction to algebraic K-theory" (Princeton, 1971); in that appendix, Milnor proves a theorem of Moore that is not algorithmic at all but of which the proof given by Milnor is algorithmically very useful; but some additional techniques also come in, especially in the non-quadratic case (which I hardly discussed). Moore's theorem is also behind the "uniqueness statements" about the norm residue symbol that I alluded to in my lecture. For the quadratic case, you will find in https://wstein.org/edu/2010/581d/projects/alyson_deines/CompMathHilbertSymbols.pdf an algorithm for computing the norm residue symbol that is due to John Voight and distantly related to the algorithm I sketched in my lecture; the quadratic case has also been implemented on various computer algebra systems.