The Fast Fourier Transform

Article *in* SIAM Journal on Control and Optimization · January 2007

DOI: 10.1137/060658242 · Source: DBLP

CITATIONS
46

READS
14,531

1 author:

Ulrich Oberst
University of Innsbruck
87 PUBLICATIONS **1,350** CITATIONS

SEE PROFILE

SIAM J. CONTROL OPTIM.
Vol. 0, No. 0, pp. 000–000

THE FAST FOURIER TRANSFORM*

ULRICH OBERST†

Abstract. Fast Fourier transforms (FFTs) are fast algorithms, i.e., of low complexity, for the computation of the discrete Fourier transform (DFT) on a finite abelian group. They are among the most important algorithms in applied and engineering mathematics and in computer science, in particular for one- and multidimensional systems theory and signal processing. We give a relatively short survey of the FFT for arbitrary finite abelian groups, cyclic or not, with complete and partially novel proofs, the main distinction being explicit induction formulas for the FFT in all cases which generalize the original FFT-algorithm due to Cooley and Tukey and, much earlier, to Gauß. We believe that our approach has didactic advantages over the usual ones. We also present the application of the FFT to fast convolution algorithms, and the so-called number theoretic transforms over finite coefficient rings. We do not treat those algorithms which decrease the multiplicative complexity at the expense of many more rational linear combinations, which in this context are considered costless, nor do we discuss the DFT for nonabelian finite groups.

Key words. fast Fourier transform, discrete Fourier transform, fast convolution

AMS subject classification. 65T50

DOI. 10.1137/060658242

1. Introduction.

Fast Fourier transforms (FFTs) are fast algorithms, i.e., of low complexity, for the computation of the *discrete Fourier transform* (DFT) on a finite abelian group which, in turn, is a special case of the Fourier transform on a locally compact abelian group. The FFTs are among the most important algorithms in applied and engineering mathematics and in computer science, in particular for *one- and multidimensional systems theory and signal processing* as evidenced by references [4], [11], [15], [19], [23], [26], [28], [34], [35], [40]. Various textbooks on the FFT are mentioned at the end of this introduction.

The present article gives a relatively *short* survey of the FFT for arbitrary finite abelian groups, cyclic or not, with complete and partially novel proofs which in our opinion have didactic advantages over the usual ones. The main distinction consists in *explicit induction formulas* for the FFT, proven and announced in 1988 [30], [31], for all possible cases which generalize the FFT-algorithm on the group $\mathbb{Z}/\mathbb{Z}2^r$ due to Cooley and Tukey [18] and, much earlier, to Gauß. We also treat the applications of the FFT to fast convolution algorithms. We do not discuss the algorithms with fewer *essential multiplications* at the expense of many more rational linear combinations, i.e., those with low *multiplicative complexity*, for instance, those of Winograd [43]. Nor do we treat the FFT for *noncommutative* finite groups [5], [13].

An algorithm is called *fast* if it has *low complexity*, where the complexity is the number of elementary computation steps necessary to execute it. In this paper and in most computer processors such a step is of the form $ax + y$ with numbers a, x, y; i.e., it consists of one multiplication together with one addition.

The following *motivational* remarks taken from [6] and [24] on the Fourier theory for general locally compact abelian groups or *harmonic analysis* will not be used in

*Received by the editors April 26, 2006; accepted for publication (in revised form) October 31, 2006; published electronically DATE.
http://www.siam.org/journals/sicon/x-x/65824.html
†Institut für Mathematik der Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria (Ulrich.Oberst@uibk.ac.at).

any way in the rest of this article. For the group $G = \mathbb{R}^r$ the *Fourier transform* of a function $a \in \mathrm{L}^1(\mathbb{R}^r)$ is the bounded, continuous function

$$\widehat{a}(y) := \int_{\mathbb{R}^r} a(x) \exp(-2\pi i x \bullet y) dx,\ y \in \mathbb{R}^r,\ \text{where } x \bullet y := x_1 y_1 + \cdots + x_r y_r$$

is the standard scalar product. Under suitable assumptions, for instance, if $\widehat{a}$ is absolutely integrable, too [22, p. 164], the *Fourier inversion formula*

$$a(x) = \int_{\mathbb{R}^r} \widehat{a}(y) \exp(+2\pi i x \bullet y) dy$$

holds almost everywhere. For fixed y the map $x \mapsto \langle x, y\rangle := \exp(-2\pi i x \bullet y)$ is a character on $\mathbb{R}^r$, i.e., a continuous group homomorphism from $\mathbb{R}^r$ into the circle group $\mathrm{S}^1 := \{z \in \mathbb{C};\ |\ z\ | = 1\}$. Let $\mathrm{Gr}_{\mathrm{cont}}(\mathbb{R}^r, \mathrm{S}^1)$ denote the multiplicative group of all characters with the multiplication of functions. Then, more precisely, the continuous, symmetric, bimultiplicative form $\langle -, -\rangle$ is nondegenerate, i.e., induces the (topological) isomorphism

$$\mathbb{R}^r \cong \mathrm{Gr}_{\mathrm{cont}}(\mathbb{R}^r, \mathrm{S}^1),\ y \mapsto \langle -, y\rangle,$$

and the Fourier inversion has the form

$$\begin{gathered}\widehat{a}(y) := \int_{\mathbb{R}^r} a(x)\langle x, y\rangle dx,\\ a(x) := \int_{\mathbb{R}^r} \widehat{a}(y)\langle -x, y\rangle dy,\ \langle -x, y\rangle = \langle x, y\rangle^{-1} = \overline{\langle x, y\rangle}.\end{gathered}$$

In general, the character group $\widehat{G} := \mathrm{Gr}_{\mathrm{cont}}(G, \mathrm{S}^1)$ of a locally compact abelian group G is not isomorphic to G, for instance, $\widehat{\mathbb{Z}^r} \cong (\mathrm{S}^1)^r$, but the form $\langle -, -\rangle : G \times \widehat{G} \to \mathrm{S}^1,\ \langle g, \widehat{g}\rangle := \widehat{g}(g)$, is nondegenerate in the sense that the map $G \to \mathrm{Gr}_{\mathrm{cont}}(\widehat{G}, \mathrm{S}^1),\ g \mapsto \langle g, -\rangle$, is a (topological) isomorphism and the Fourier inversion has the form

$$\begin{gathered}\widehat{a}(\widehat{g}) := \int_G a(g)\langle g, \widehat{g}\rangle dg,\ a \in \mathrm{L}^1(G),\\ a(g) := \int_{\widehat{G}} \widehat{a}(\widehat{g})\langle -g, \widehat{g}\rangle d\widehat{g},\ \langle -g, \widehat{g}\rangle = \langle g, \widehat{g}\rangle^{-1} = \overline{\langle g, \widehat{g}\rangle},\end{gathered}$$

where dg, respectively, $d\widehat{g}$, are the suitably normalized *Haar measures* on G, respectively, $\widehat{G}$.

We specialize the preceding considerations to the simple case of a finite abelian group G of exponent $d > 0$, i.e., satisfying $dG = 0$. In various ways one can choose a group $\widehat{G} \cong G$, for instance, $\widehat{G} = G$, and a biadditive form

$$\begin{gathered}\bullet : G \times \widehat{G} \to \mathbb{Z}/\mathbb{Z}d \text{ such that}\\ \widehat{G} \cong \mathrm{Hom}(G, \mathbb{Z}/\mathbb{Z}d),\ \widehat{g} \mapsto (-) \bullet \widehat{g},\ \text{and } G \cong \mathrm{Hom}(\widehat{G}, \mathbb{Z}/\mathbb{Z}d),\ g \mapsto g \bullet (-),\end{gathered}$$

are isomorphisms, the latter signifying that the form $\bullet$ is *nondegenerate*. In the engineering literature the groups G and $\widehat{G}$ are called the *time*, respectively, the *frequency* domain, in the standard one-dimensional case of time signals. We choose a primitive dth root of one in $\mathbb{C}$, for instance, $\zeta := \exp(-\frac{2\pi i}{d})$; hence

$$\mathbb{Z}/\mathbb{Z}d \cong \mu := \langle\zeta\rangle = \{1, \zeta, \cdots, \zeta^{d-1}\} \subseteq \mathrm{S}^1, \overline{k} \mapsto \zeta^{\overline{k}} := \zeta^k.$$

The nondegenerate form $\bullet$ thus induces the nondegenerate bimultiplicative form

$$\begin{gathered}\langle -, -\rangle : G \times \widehat{G} \to \mu,\ \langle g, \widehat{g}\rangle := \zeta^{g \bullet \widehat{g}},\ \text{such that}\\ \widehat{G} \cong \mathrm{Gr}(G, \mu),\ \widehat{g} \mapsto \langle -, \widehat{g}\rangle,\ \text{and } G \cong \mathrm{Gr}(\widehat{G}, \mu),\ g \mapsto \langle g, -\rangle.\end{gathered}$$

Here $\mathrm{Gr}(G,\mu)$ denotes the *multiplicative* abelian group of homomorphisms from the *additive* abelian group G into the *multiplicative* abelian group μ. The canonical group isomorphisms

$$\widehat{G} \cong \mathrm{Hom}(G, \mathbb{Z}/\mathbb{Z}d) \cong \mathrm{Gr}(G,\mu) = \mathrm{Gr}(G, \mathrm{S}^1)$$

hold. In this article we use the chosen group $\widehat{G}$ instead of the isomorphic *character group* $\mathrm{Gr}(G,\mu)$ for the development of the theory. The standard choices for the one-dimensional DFT are

$$d > 0,\ G := \widehat{G} = \mathbb{Z}/\mathbb{Z}d,\ \overline{k} \bullet \overline{l} = \overline{kl},\ \langle \overline{k}, \overline{l} \rangle = \exp\left(-2\pi i \tfrac{kl}{d}\right).$$

It is a well-known and simple, but for this paper essential, observation that the contravariant *duality functor* $G \mapsto \widehat{G} \cong \mathrm{Gr}(G,\mu)$ is exact on finite abelian groups of exponent d. The Haar integral on $\mathbb{C}^G$ which is unique up to a multiplicative positive constant is the map $\mathbb{C}^G \to \mathbb{C},\ a \mapsto \sum_{g\in G} a(g)$. Therefore we define two DFTs

$$\begin{aligned} \mathrm{Four}_G : \mathbb{C}^G \to \mathbb{C}^{\widehat{G}},\ a \mapsto \widehat{a},\ \widehat{a}(\widehat{g}) := \textstyle\sum_{g\in G} a(g)\langle g, \widehat{g}\rangle,\ \text{and} \\ \mathrm{Four}_{\widehat{G}} : \mathbb{C}^{\widehat{G}} \to \mathbb{C}^G,\ b \mapsto \widehat{b},\ \widehat{b}(g) := \textstyle\sum_{\widehat{g}\in\widehat{G}} b(\widehat{g})\langle g, \widehat{g}\rangle. \end{aligned}$$

The map $\mathrm{Four}_{\widehat{G}}$ is sometimes called the *inverse discrete Fourier transform* (IDFT). The Fourier inversion formula has the form

$$N^{-1}\widehat{\widehat{a}}(-g) = a(g),\ \text{where } a \in \mathbb{C}^G,\ N := \mathrm{ord}(G).$$

The form $\langle -, - \rangle$ and the Fourier transform can also be defined if $\mathbb{C}$ is replaced by an arbitrary commutative ring K and if ζ is a primitive dth root of one in K, and we will do this in these notes. However, the Fourier inversion holds under additional assumptions on ζ only [29], [16], [20]. Interesting cases concern finite factor rings $K = \mathbb{Z}/\mathbb{Z}M$ of $\mathbb{Z}$, where the corresponding DFT is also called a *number theoretic transform* (NTT), or rings of algebraic integers. In our opinion the change of the coefficient ring does not justify a change of the terminology, so we will always talk of the DFT.

Any filtration or increasing sequence of subgroups $0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G$ of G gives rise to an FFT-algorithm for the computation of Four_G. That nontrivial subgroups H of G and their factor groups G/H are significant for the construction of an FFT for Four_G is one of the basic observations in this field since [18], and the book [5], for instance, stresses this point of view. For groups of prime order there are no FFTs *in this sense*, and different algorithms have been designed, the first one by Rader [36]. Our description of the recursive FFT-algorithms gives simple explicit recursion formulas and makes essential use of the exactness of the duality functor. For the important case of cyclic groups similar formulas are contained in [8, pp. 188–191].

The central and novel sections of this survey paper are those on the FFT. The sections on duality theory, the DFT, and the complexity of linear maps contain necessary preliminaries and are simple adaptions from the literature. The two short sections on fast convolution algorithms derived from the FFT and on NTTs are included for completeness' sake and are also simple variants of the literature [29].

Since the FFT is so important in engineering applications there are very many papers and books on this subject, too numerous to be available to and be read and known by the author. Therefore the list of references at the end of this survey paper contains only books and papers which are actually mentioned in the text, and omission

of an article is no comment whatsoever on its historical or practical significance. Standard textbooks on the FFT are those of Brigham [8], Nussbaumer [29], and Beth [5] (in German), newer books are those of Clausen and Baum [13], Chu and George [14], and Garg [20]. Besides the signal processing and systems textbooks quoted above, the book [8] and especially that of Briggs and Henson [7] give surveys of the many mathematical and technical applications of the DFT and thus of the FFT from an engineering point of view, for instance, to the computation of Fourier integrals and coefficients, to trigonometric interpolation, and to digital filtering.

We shortly discuss the literature on the construction of FFT and convolution algorithms which minimize the *multiplicative complexity* according to Winograd and which are otherwise not treated in the present paper. The seminal papers in this direction are those of Winograd, Auslander, and Tolimieri and their coworkers [42], [43], [2], [1], [38]. In [32], [41], and the book [33], which unfortunately has not yet appeared, we constructed the *optimal* fast Fourier and Hartley, respectively, Gelfand, transforms on arbitrary finite abelian groups, respectively, finite-dimensional, commutative, semisimple $\mathbb{Q}$-algebras, i.e., algorithms for these transformations of *minimal multiplicative complexity*, and computed the exact value of the latter with the help of [3]. The recent paper [39] emphasizes the renewed interest in such algorithms.

The present paper presupposes the algebraic knowledge of a mathematics student at the end of the second university year. Some results are recalled under the title *Reminder*.

2. Duality.

Reminder 1 (see [25, p. 46]). Let $G = (G, +)$ be a finite abelian group, written additively. Then there are numbers $d_1 > 0, \cdots, d_r > 0$ and an isomorphism

$$G \cong \mathbb{Z}/\mathbb{Z}d_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}d_r. \tag{1}$$

The least common multiple

$$\exp(G) := \operatorname{lcm}(d_1, \cdots, d_r) \text{ with } \mathbb{Z}\exp(G) = \{k \in \mathbb{Z};\ kG = 0\} \tag{2}$$

is called *the exponent* of G. If, in addition, d_ϱ divides $d_{\varrho+1}$ for all $\varrho = 1, \cdots, r-1$, then the d_ϱ are unique and are called the *invariant factors* of G and $\exp(G) = d_r$. If d is a multiple of $\exp(G)$ or, in other terms, if $dG = 0$, we say that G is a *group of exponent* d.

If G and H are additively written abelian groups, the group of all additive or $\mathbb{Z}$-linear homomorphisms from G to H is denoted by $\operatorname{Hom}(G, H) = \operatorname{Hom}_{\mathbb{Z}}(G, H)$ as usual.

If $r > 0$ and K is a field, the map

$$\bullet : K^r \times K^r \to K,\ x \bullet y := x_1y_1 + \cdots + x_ry_r \text{ for } x = (x_1, \cdots, x_r),$$

is a nondegenerate symmetric bilinear form; i.e., the induced map

$$K^r \to \operatorname{Hom}_K(K^r, K),\ y \mapsto (-) \bullet y = y \bullet (-),$$

is a K-isomorphism.

The following symmetric bilinear form is the analogue of the preceding one for finite abelian groups.

THEOREM 2 (nondegenerate bilinear form). *Let*

$$G = \mathbb{Z}/\mathbb{Z}d_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}d_r \ni g = (\overline{g_1}, \cdots, \overline{g_r}),\ g_\varrho \in \mathbb{Z},$$

be the finite abelian group of exponent $d > 0$, i.e., $dG = 0$. Then the map

$$\bullet : G \times G \to \mathbb{Z}/\mathbb{Z}d,\ g \bullet h := \overline{\textstyle\sum_{\varrho=1}^{r} g_\varrho h_\varrho \frac{d}{d_\varrho}}, \tag{3}$$

is well defined and is a nondegenerate, symmetric $\mathbb{Z}$-bilinear form; i.e., the following hold.

(1) *The definition is independent of the representatives g_ϱ, h_ϱ.*
(2) *$g \bullet h = h \bullet g,\ g \bullet (h + h') = g \bullet h + g \bullet h'$ for all g, h, h' in G.*
(3) *$G \cong \mathrm{Hom}(G, \mathbb{Z}/\mathbb{Z}d),\ h \mapsto (-) \bullet h$.*

Proof. (1) *The map is well defined*: Let $g = (\overline{g_1}, \cdots, \overline{g_r}) = (\overline{g'_1}, \cdots, \overline{g'_r})$; hence $g'_\varrho = g_\varrho + k_\varrho d_\varrho,\ k_\varrho \in \mathbb{Z}$, for $\varrho = 1, \cdots, r$. But then

$$\textstyle\sum_{\varrho=1}^{r} g'_\varrho h_\varrho \frac{d}{d_\varrho} = \sum_{\varrho=1}^{r} g_\varrho h_\varrho \frac{d}{d_\varrho} + \sum_{\varrho=1}^{r} g_\varrho h_\varrho k_\varrho d \in \sum_{\varrho=1}^{r} g_\varrho h_\varrho \frac{d}{d_\varrho} + \mathbb{Z}d, \text{ and hence}$$
$$\overline{\textstyle\sum_{\varrho=1}^{r} g'_\varrho h_\varrho \frac{d}{d_\varrho}} = \overline{\textstyle\sum_{\varrho=1}^{r} g_\varrho h_\varrho \frac{d}{d_\varrho}} = g \bullet h.$$

The independence of the representatives h_ϱ is shown in the same fashion.

(2) The symmetry and bilinearity follow trivially from the definition.

(3) It remains to show that $G \to \mathrm{Hom}(G, \mathbb{Z}/\mathbb{Z}d),\ h \bullet (-) = (-) \bullet h$, is an isomorphism.

(i) *Monomorphism*: Assume that $(-) \bullet h = 0$. For $\varrho = 1, \cdots, r$ let $\delta_\varrho := (0, \cdots, 0, \overset{\varrho}{\overline{1}}, 0, \cdots, 0)$ denote the analogue of the standard basis such that $(\overline{g_1}, \cdots, \overline{g_r}) = \sum_{\varrho=1}^{r} g_\varrho \delta_\varrho$ for all $g \in G$. Then

$$0 = \delta_\varrho \bullet h = \overline{h_\varrho \tfrac{d}{d_\varrho}} \in \mathbb{Z}/\mathbb{Z}d; \text{ hence for } \varrho = 1, \cdots, r$$
$$d \mid h_\varrho \tfrac{d}{d_\varrho} \text{ or } d_\varrho \mid h_\varrho \text{ and } \overline{h_\varrho} = 0 \text{ in } \mathbb{Z}/\mathbb{Z}d_\varrho, \text{ i.e., } h = 0.$$

(ii) *Epimorphism*: Let $\varphi : G \to \mathbb{Z}/\mathbb{Z}d$ be any homomorphism. The equation

$$d_\varrho \delta_\varrho = 0 \text{ implies } d_\varrho \varphi(\delta_\varrho) = 0 \text{ in } \mathbb{Z}/\mathbb{Z}d; \text{ hence } \varphi(\delta_\varrho) = \overline{h_\varrho \tfrac{d}{d_\varrho}} = \delta_\varrho \bullet h,\ h_\varrho \in \mathbb{Z},$$
$$\text{and for } g \in G : \ \varphi(g) = \varphi(\textstyle\sum_{\varrho=1}^{r} g_\varrho \delta_\varrho) = \sum_{\varrho=1}^{r} g_\varrho \varphi(\delta_\varrho)$$
$$= \textstyle\sum_{\varrho=1}^{r} g_\varrho \delta_\varrho \bullet h = (\sum_{\varrho=1}^{r} g_\varrho \delta_\varrho) \bullet h = g \bullet h \text{ and } \varphi = (-) \bullet h. \qquad \square$$

Corollary 3. *With the data of the preceding theorem, let G_1 and G_2 be two groups which are isomorphic to G and let $\varphi_i : G_i \cong G,\ i = 1, 2$, be two isomorphisms. Then*

$$\bullet : G_1 \times G_2 \to \mathbb{Z}/\mathbb{Z}d,\ g_1 \bullet g_2 := \varphi_1(g_1) \bullet \varphi_2(g_2), \tag{4}$$

is a nondegenerate bilinear form; i.e., the maps

$$G_1 \to \mathrm{Hom}(G_2, \mathbb{Z}/\mathbb{Z}d),\ g_1 \mapsto g_1 \bullet (-), \quad \textit{and} \quad G_2 \to \mathrm{Hom}(G_1, \mathbb{Z}/\mathbb{Z}d),\ g_2 \mapsto (-) \bullet g_2,$$

are isomorphisms.

The proof is obvious. The corollary implies that the following assumptions can be realized in various ways.

Assumption 4. Let $d > 0$. In what follows we consider finite abelian groups G with $dG = 0$. For each such G we choose a group $\widehat{G}$ and a nondegenerate bilinear form $\bullet : G \times \widehat{G} \to \mathbb{Z}/\mathbb{Z}d$, hence the *canonical* isomorphisms

$$\mathrm{can} : G \cong \mathrm{Hom}(\widehat{G}, \mathbb{Z}/\mathbb{Z}d),\ g \mapsto g \bullet (-), \text{ and } \mathrm{can} : \widehat{G} \cong \mathrm{Hom}(G, \mathbb{Z}/\mathbb{Z}d),\ \widehat{g} \mapsto (-) \bullet \widehat{g}. \tag{5}$$

For the groups $G = \mathbb{Z}/\mathbb{Z}d_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}d_r$ the canonical choices are $\widehat{G} = G$ and the symmetric form of (3). In the context of the FFT the groups G (resp., $\widehat{G}$) are often called the *time domain* (resp., the *frequency domain*), and therefore it is advantageous to make a notational distinction between G and $\widehat{G}$ even if $G = \widehat{G}$.

If G is any finite abelian group the theory applies for $d = \exp(G)$.

Reminder 5 (see [25, pp. 76,77]). $\mathrm{Hom}(G, H)$ is an *additive functor* in its two variables G and H. In particular, a homomorphism $\varphi : G_1 \to G_2$ of abelian groups induces the homomorphism

$$\mathrm{Hom}(\varphi, \mathbb{Z}/\mathbb{Z}d) : \mathrm{Hom}(G_2, \mathbb{Z}/\mathbb{Z}d) \to \mathrm{Hom}(G_1, \mathbb{Z}/\mathbb{Z}d),\ \chi_2 \mapsto \chi_2\varphi,$$

in the reverse direction. This assignment satisfies the relations

$$\begin{gathered}\mathrm{Hom}(\mathrm{id}_G, \mathbb{Z}/\mathbb{Z}d) = \mathrm{id}_{\mathrm{Hom}(G,\mathbb{Z}/\mathbb{Z}d)},\\ \mathrm{Hom}(\varphi_1, \mathbb{Z}/\mathbb{Z}d)\,\mathrm{Hom}(\varphi_2, \mathbb{Z}/\mathbb{Z}d) = \mathrm{Hom}(\varphi_2\varphi_1, \mathbb{Z}/\mathbb{Z}d) \text{ for } G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3,\\ \mathrm{Hom}(\varphi^{-1}, \mathbb{Z}/\mathbb{Z}d) = \mathrm{Hom}(\varphi, \mathbb{Z}/\mathbb{Z}d)^{-1} \text{ if } \varphi : G_1 \cong G_2.\end{gathered}$$

Corollary 6. *For each finite abelian group G of exponent $d > 0$ there is a* noncanonical *isomorphism $G \cong \widehat{G}$.*

Proof. Choose an isomorphism $\varphi : H = \mathbb{Z}/\mathbb{Z}d_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}d_r \to G$ and on H the bilinear form from (3) which induces the isomorphism $H \cong \mathrm{Hom}(H, \mathbb{Z}/\mathbb{Z}d)$. Then

$$\widehat{G} \cong \mathrm{Hom}(G, \mathbb{Z}/\mathbb{Z}d) \overset{\mathrm{Hom}(\varphi,\mathbb{Z}/\mathbb{Z}d)}{\cong} \mathrm{Hom}(H, \mathbb{Z}/\mathbb{Z}d) \cong H \cong G. \qquad \square$$

Remark 7. If K is a field, V a finite-dimensional K-vector space, and $V^\star := \mathrm{Hom}_K(V, K)$ its dual space, the canonical Gelfand map

$$\mathrm{Gelf} : V \to V^{\star\star},\ v \mapsto \mathrm{Gelf}(v),\ \mathrm{Gelf}(v)(v^\star) := v^\star(v),$$

is a K-isomorphism. The following result is the analogue for finite abelian groups.

Theorem 8. *There is the unique* canonical Gelfand *isomorphism*

$$\mathrm{Gelf}_G : G \cong \widehat{\widehat{G}} \text{ with } g \bullet \widehat{g} = \widehat{g} \bullet \mathrm{Gelf}_G(g) \text{ for all } g \in G,\ \widehat{g} \in \widehat{G}. \tag{6}$$

Proof.

$$G \cong \mathrm{Hom}(\widehat{G}, \mathbb{Z}/\mathbb{Z}d) \cong \widehat{\widehat{G}},\ g \to g \bullet (-) = (-) \bullet \mathrm{Gelf}_G(g) \leftarrow \mathrm{Gelf}_G(g). \qquad \square$$

Lemma and Definition 9. 1. *For each homomorphism $\varphi : G_1 \to G_2$ there is a unique homomorphism*

$$\varphi^\star : \widehat{G_2} \to \widehat{G_1} \text{ such that } \varphi(g_1) \bullet \widehat{g_2} = g_1 \bullet \varphi^\star(\widehat{g_2}) \text{ for all } g_1 \in G_1,\ \widehat{g_2} \in \widehat{G_2}. \tag{7}$$

The map $\varphi^\star$ is called the adjoint *of φ.*

2. The relations $\mathrm{id}_G^\star = \mathrm{id}_{\widehat{G}}$ and $\varphi_1^\star\varphi_2^\star = (\varphi_2\varphi_1)^\star$ for $G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3$ hold.

Hence the assignment $G \mapsto \widehat{G},\ \varphi \mapsto \varphi^\star$, is a contravariant functor on finite abelian groups of exponent $d > 0$ and is called the duality functor *in this article. Observe that $\widehat{G} \cong \mathrm{Hom}(G, \mathbb{Z}/\mathbb{Z}d)$ can be chosen in various ways.*

Proof. 1. There is a unique homomorphism $\varphi^\star$ such that the following diagram with vertical isomorphisms is commutative:

$$
\begin{array}{ccc}
\widehat{G_2} & \xrightarrow{\varphi^\star} & \widehat{G_1} \\
\downarrow \text{ can}_2 & & \downarrow \text{ can}_1 \\
\text{Hom}(G_2, \mathbb{Z}/\mathbb{Z}d) & \xrightarrow{\text{Hom}(\varphi, \mathbb{Z}/\mathbb{Z}d)} & \text{Hom}(G_1, \mathbb{Z}/\mathbb{Z}d) \\
\widehat{g_2} & \mapsto & \varphi^\star(\widehat{g_2}) \\
\downarrow & & \downarrow \\
\chi_2 := (-) \bullet \widehat{g_2} & \mapsto & \chi_2\varphi = \varphi(-) \bullet \widehat{g_2} = (-) \bullet \varphi^\star(\widehat{g_2})
\end{array}
\tag{8}
$$

viz., $\varphi^\star := \text{can}_1^{-1} \circ \text{Hom}(\varphi, \mathbb{Z}/\mathbb{Z}d) \circ \text{can}_2$. The commutativity signifies that

$$\varphi(g_1) \bullet \widehat{g_2} = g_1 \bullet \varphi^\star(\widehat{g_2}) \text{ for all } g_1 \in G_1,\ \widehat{g_2} \in \widehat{G_2}.$$

2. The relations follow from the commutative diagram (8) and from Reminder 5. ∎

LEMMA 10. *The Gelfand map is a natural transformation; i.e., for $\varphi : G_1 \to G_2$ the following diagram is commutative:*

$$
\begin{array}{ccc}
G_1 & \xrightarrow{\varphi} & G_2 \\
\downarrow \text{ Gelf}_1 & & \downarrow \text{ Gelf}_2 \\
\widehat{\widehat{G_1}} & \xrightarrow{\varphi^{\star\star}} & \widehat{\widehat{G_2}}
\end{array}
\ .
\tag{9}
$$

Proof. For all $g_1 \in G_1$ and $\widehat{g_2} \in \widehat{G_2}$ we have

$$
\begin{gathered}
\widehat{g_2} \bullet \text{Gelf}_2(\varphi(g_1)) = \varphi(g_1) \bullet \widehat{g_2} = g_1 \bullet \varphi^\star(\widehat{g_2}) \\
= \varphi^\star(\widehat{g_2}) \bullet \text{Gelf}_1(g_1) = \widehat{g_2} \bullet \varphi^{\star\star}(\text{Gelf}_1(g_1)); \text{ hence} \\
\text{Gelf}_2(\varphi(g_1)) = \varphi^{\star\star}(\text{Gelf}_1(g_1)).
\end{gathered}
$$ ∎

Reminder 11 (exactness, [25, pp. 16, 77]). 1. Consider a sequence of abelian groups and homomorphisms

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3. \tag{10}$$

The sequence is called a *complex* if $\varphi_2\varphi_1 = 0$ or $\text{im}(\varphi_1) \subseteq \ker(\varphi_2)$.

2. The sequence (10) is called *exact* if $\text{im}(\varphi_1) = \ker(\varphi_2)$.

3. A possibly infinite sequence

$$G_* : \ \cdots \to G_{i+1} \xrightarrow{d_{i+1}} G_i \xrightarrow{d_i} G_{i-1} \to \cdots, i \in \mathbb{Z}, \tag{11}$$

is called a *complex* (resp., *exact*) if and only if all three member subsequences have this property, i.e. $B_i := \text{im}(d_{i+1}) \subseteq Z_i := \ker(d_i)$ (resp., $B_i = Z_i$) for all i. The groups $H_i(G_*) := Z_i/B_i$ are called the *homology groups* of the complex and are all zero if and only if G_* is exact.

4. For a sequence

$$0 \longrightarrow G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \tag{12}$$

the following properties are equivalent.

(a) The sequence is exact.

(b) $\ker(\varphi_1) = 0$, i.e., φ_1 is a monomorphism, and $\operatorname{im}(\varphi_1) = \ker(\varphi_2)$.
(c) The map φ_1 induces an isomorphism $\varphi_{1,\mathrm{ind}} : G_1 \cong \ker(\varphi_2)$.

5. For a sequence

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \longrightarrow 0 \tag{13}$$

and the *cokernel* $\operatorname{cok}(\varphi_1) := G_2/\operatorname{im}(\varphi_1)$ the following properties are equivalent.
(a) The sequence is exact.
(b) $\operatorname{im}(\varphi_2) = G_3$, i.e., φ_2 is an epimorphism, and $\operatorname{im}(\varphi_1) = \ker(\varphi_2)$.
(c) The map φ_2 induces the isomorphism $\varphi_{2,\mathrm{ind}} : \operatorname{cok}(\varphi_1) \cong G_3$, $\overline{g_2} \mapsto \varphi_2(g_2)$.

6. The Hom-functor is left exact. Moreover, the sequence (13) is exact if and only if for all abelian groups X the derived sequence

$$\operatorname{Hom}(G_1, X) \xleftarrow{\operatorname{Hom}(\varphi_1, X)} \operatorname{Hom}(G_2, X) \xleftarrow{\operatorname{Hom}(\varphi_2, X)} \operatorname{Hom}(G_3, X) \longleftarrow 0 \tag{14}$$

is exact.

The next *duality theorem* states that the duality functor $G \mapsto \widehat{G}$ preserves and reflects exactness.

THEOREM 12 (duality theorem). *A sequence*

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \tag{15}$$

of finite abelian groups G of exponent d ($dG = 0$) is exact if and only if its dual sequence

$$\widehat{G_1} \xleftarrow{\varphi_1^\star} \widehat{G_2} \xleftarrow{\varphi_2^\star} \widehat{G_3} \tag{16}$$

has this property.

Proof. $\Rightarrow$: 1. Assume first that the sequence

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \longrightarrow 0 \tag{17}$$

is exact, i.e., φ_2 is surjective. Lemma 9 implies the commutative diagram

$$\begin{array}{ccccccccc}
\widehat{G_1} & & \xleftarrow{\varphi_1^\star} & & \widehat{G_2} & \xleftarrow{\varphi_2^\star} & \widehat{G_3} & \leftarrow & 0 \\
\downarrow \mathrm{can}_1 & & & & \downarrow \mathrm{can}_2 & & \downarrow \mathrm{can}_3 & & \\
\operatorname{Hom}(G_1, \mathbb{Z}/\mathbb{Z}d) & & \xleftarrow{\operatorname{Hom}(\varphi_1, \mathbb{Z}/\mathbb{Z}d)} & & \operatorname{Hom}(G_2, \mathbb{Z}/\mathbb{Z}d) & \xleftarrow{\operatorname{Hom}(\varphi_2, \mathbb{Z}/\mathbb{Z}d)} & \operatorname{Hom}(G_3, \mathbb{Z}/\mathbb{Z}d) & \leftarrow & 0
\end{array}$$

with vertical isomorphisms whose lower row is exact according to part 6 of Reminder 11. The commutativity then implies that also the upper row is exact.

2. We prove that $\varphi^\star$ is an epimorphism if $\varphi : G_1 \to G_2$ is a monomorphism.

The sequence

$$0 \leftarrow C := \operatorname{cok}(\varphi^\star) \xleftarrow{\mathrm{can}} \widehat{G_1} \xleftarrow{\varphi^\star} \widehat{G_2}$$

is exact. Part 1 of this proof and Lemma 10 imply the commutative diagram

$$\begin{array}{ccccccc}
 & & & & G_1 & \xrightarrow{\varphi} & G_2 \\
 & & & & \downarrow \mathrm{Gelf}_1 & & \downarrow \mathrm{Gelf}_2 \\
0 & \to & \widehat{C} & \xrightarrow{\mathrm{can}^\star} & \widehat{\widehat{G_1}} & \xrightarrow{\varphi^{\star\star}} & \widehat{\widehat{G_2}}
\end{array}$$

with exact row and vertical isomorphisms. Since φ is a monomorphism, so is $\varphi^{\star\star}$, and hence $\widehat{C} = 0$. Since C and $\widehat{C}$ are isomorphic, we obtain $C = \operatorname{cok}(\varphi^\star) = 0$ or that $\varphi^\star$ is surjective.

3. The exact sequence (15) gives rise to the commutative diagram

$$\begin{array}{ccccccc} G_1 & \xrightarrow{\varphi_1} & G_2 & \xrightarrow{\mathrm{can}} & C := \operatorname{cok}(\varphi_1) & \longrightarrow & 0 \\ & & \downarrow\ \varphi_2 & & \downarrow\ \psi & & \\ & & G_3 & = & G_3 & & \end{array},$$

where $\psi(\overline{g_2}) = \varphi_2(g_2)$. Since $C = G_2/\operatorname{im}(\varphi_1) = G_2/\ker(\varphi_2)$, the homomorphism theorem implies that ψ is a monomorphism. Dual to the preceding one is the commutative diagram

$$\begin{array}{ccccccc} \widehat{G_1} & \xleftarrow{\varphi_1^\star} & \widehat{G_2} & \xleftarrow{\mathrm{can}^\star} & \widehat{C} & \longleftarrow & 0 \\ & & \uparrow\ \varphi_2^\star & & \uparrow\ \psi^\star & & \\ & & \widehat{G_3} & = & \widehat{G_3} & & \end{array}.$$

Its first row is exact, and $\psi^\star$ is an epimorphism according to parts 1 and 2 of the proof. Since $\varphi_2^\star = \mathrm{can}^\star\,\psi^\star$, we conclude that $\operatorname{im}(\varphi_2^\star) = \operatorname{im}(\mathrm{can}^\star) = \ker(\varphi_1^\star)$ and thus the exactness of (16).

$\Leftarrow$: Assume that (16) is exact. There results the diagram

$$\begin{array}{ccccc} G_1 & \xrightarrow{\varphi_1} & G_2 & \xrightarrow{\varphi_2} & G_3 \\ \downarrow\ \mathrm{Gelf}_1 & & \downarrow\ \mathrm{Gelf}_2 & & \downarrow\ \mathrm{Gelf}_3 \\ \widehat{\widehat{G_1}} & \xrightarrow{\varphi_1^{\star\star}} & \widehat{\widehat{G_2}} & \xrightarrow{\varphi_2^{\star\star}} & \widehat{\widehat{G_3}} \end{array}.$$

The exactness of (16) and the proof "$\Rightarrow$" imply the exactness of its lower row, and Lemma 10 implies its commutativity. Since the Gelfand maps are isomorphisms, the wanted exactness of the upper row follows. □

3. The discrete Fourier transform. In this section we define and investigate the DFT for K-valued functions on a *finite* abelian group where K denotes a suitable coefficient field or even ring.

Assumption 13. The assumptions of section 2 remain in force, in particular $d > 0$. We consider finite additively written abelian groups G of exponent d ($dG = 0$) and the nondegenerate bilinear forms $\bullet : G \times \widehat{G} \to \mathbb{Z}/\mathbb{Z}d$. Let K be a commutative *coefficient* ring. Then K^G is the K-module of functions from G to K with its argumentwise addition and scalar multiplication. The standard case for the FFT will be the coefficient field $\mathbb{C}$ of complex numbers. However, since we are also going to discuss the so-called arithmetic transforms with a finite coefficient ring or field, we consider the more general situation from Assumption 13. Let $\mathrm{U}(K)$ denote the group of units or invertible elements of K. For the definition of the DFT on K^G we also need an analogue of the circle group $S^1 = \{z \in \mathbb{C};\ |\ z\ |= 1\} \subset \mathrm{U}(\mathbb{C})$ in the standard case of complex Fourier transforms. Therefore we make the following additional assumption for the ring K.

Assumption 14. Let $\zeta \in \mathrm{U}(K)$ be a *primitive dth root of one* in K, i.e.

$$\zeta^d = 1,\ \mu := \langle\zeta\rangle = \{1, \zeta, \cdots, \zeta^{d-1}\} \subseteq \mathrm{U}(K),\ \operatorname{ord}(\zeta) = \operatorname{ord}(\mu) = d.$$

Examples 15.

(1) Let

$$K := \mathbb{C},\ \zeta := \exp\left(-\tfrac{2\pi i}{d}\right). \text{ Then } \mu := \langle\zeta\rangle = \{\eta \in \mathbb{C};\ \eta^d = 1\}$$

is the group of *all* dth roots of one in $\mathbb{C}$ and consists of the vertices of the regular d-gon. These data are those of the standard complex DFT.

(2) Let $d := 2,\ K := \mathbb{R},\ \zeta := -1$. These data are used for the discrete *Walsh–Fourier* transform.

(3) Let $K := \mathbb{C} \times \mathbb{C},\ \zeta := (\zeta_1, \zeta_2) := (\exp(-\frac{2\pi i}{d}), 1)$. This is a primitive dth root of one, but it does not generate the finite group of all dth roots of one which consists of the elements (ζ_1^m, ζ_1^n).

(4) Let K be a finite field of characteristic p and dimension $[K : \mathbb{Z}/\mathbb{Z}p] = n$, hence with $q := p^n$ elements. The group $\mathrm{U}(K) = K \setminus \{0\}$ is cyclic and hence generated by a primitive root of order $d := q-1$. For instance, $\mathrm{U}(\mathbb{Z}/\mathbb{Z}7) = \langle\overline{3}\rangle$, whereas $\mathrm{ord}(\overline{2}) = 3$.

If G_1 and G_2 are arbitrary abelian groups and one of them is multiplicatively written, we denote the group of all homomorphisms from G_1 to G_2 by $\mathrm{Gr}(G_1, G_2)$ instead of $\mathrm{Hom}(G_1, G_2)$.

LEMMA 16. *Consider the situation of Example* 15(1) *and a finite abelian group* G *with* $dG = 0$. *Then* $\mathrm{Gr}(G, \mu) = \mathrm{Gr}(G, S^1)$ *is the group of all* complex characters *on* G.

Proof. Let $\chi : G \to S^1$ be any character, i.e., homomorphism. The relations $dg = 0$ for $g \in G$ imply $\chi(g)^d = 1$ and hence $\chi(g) \in \mu$ since μ is the group of *all* roots of 1. □

This result suggests that we consider the group $\mathrm{Gr}(G, \mu)$ as a suitable analogue of the character group for general coefficient rings, and we will do this; i.e, we call this group the *character group* of G. Notice that, in general, this group depends on the choice of ζ in contrast to the complex case.

COROLLARY AND DEFINITION 17. *The maps*

$$\begin{gathered}\mathbb{Z}/\mathbb{Z}d \cong \mu = \langle\zeta\rangle,\ \overline{k} \mapsto \zeta^{\overline{k}} := \zeta^k,\ \textit{hence also}\\ \mathrm{Hom}(G, \mathbb{Z}/\mathbb{Z}d) \cong \mathrm{Gr}(G, \mu),\ \varphi \mapsto \chi,\ \chi(g) = \zeta^{\varphi(g)},\end{gathered} \tag{18}$$

are isomorphisms. For each group G *(finite abelian,* $dG = 0$*) the nondegenerate bilinear form* $\bullet : G \times \widehat{G} \to \mathbb{Z}/\mathbb{Z}d$ *induces the nondegenerate bimultiplicative form*

$$\langle -, - \rangle : G \times \widehat{G} \to \mu = \langle\zeta\rangle,\ \langle g, \widehat{g}\rangle := \zeta^{g \bullet \widehat{g}};\ \textit{i.e.,} \tag{19}$$

(1) *for all* $g_1, g_2 \in G$ *and* $\widehat{g_1}, \widehat{g_2} \in \widehat{G}$

$$\langle g_1, \widehat{g_1} + \widehat{g_2}\rangle = \langle g, \widehat{g_1}\rangle\langle g, \widehat{g_2}\rangle,\ \langle g_1 + g_2, \widehat{g}\rangle = \langle g_1, \widehat{g}\rangle\langle g_2, \widehat{g}\rangle,$$

(2)

$$G \cong \mathrm{Gr}(\widehat{G}, \mu),\ g \mapsto \langle g, -\rangle,\ \widehat{G} \cong \mathrm{Gr}(G, \mu),\ \widehat{g} \mapsto \langle -, \widehat{g}\rangle.$$

The proof of this corollary is obvious since it consists in just replacing the additive group $\mathbb{Z}/\mathbb{Z}d$ by the multiplicative group $\mu = \langle\zeta\rangle$.

Reminder 18. The K-module K^G of all functions $a = (a(g))_{g\in G} : G \to K$ has the standard basis $\delta_h := (\delta_{h,g})_{g\in G},\ h \in G$, and the basis representation is

$$a = (a(g))_{g\in G} = \textstyle\sum_{g\in G} a(g)\delta_g.$$

We also consider the function module $K^{\widehat{G}}$ with the corresponding structure.

LEMMA AND DEFINITION 19 (DFT). *The data are as introduced above. The map*

$$\mathrm{Four}_G : K^G \to K^{\widehat{G}},\ a \mapsto \widehat{a},\ \widehat{a}(\widehat{g}) := \textstyle\sum_{g\in G} a(g)\langle g, \widehat{g}\rangle,$$

is K-linear and is called the discrete Fourier transform (DFT). *The function $\widehat{a} \in K^{\widehat{G}}$ is also called the Fourier transform of a. The analogous map*

$$\mathrm{Four}_{\widehat{G}} : K^{\widehat{G}} \to K^G,\ b \mapsto \widehat{b},\ \widehat{b}(g) := \textstyle\sum_{\widehat{g}\in\widehat{G}} b(\widehat{g})\langle g, \widehat{g}\rangle,$$

is called the Fourier transform *on $K^{\widehat{G}}$ or* inverse Fourier transform (IDFT). *Notice that $\mathrm{Four}_{\widehat{G}}$ maps into K^G and not into $K^{\widehat{\widehat{G}}}$.*

The Fourier transform depends on the choice of the non-degenerate form $\bullet$ and of the primitive dth root ζ.

Examples 20. (1) Let $d := n > 0$, $K := \mathbb{C}$, $\zeta := \exp(-\frac{2\pi i}{n})$, and $G := \mathbb{Z}_n := \mathbb{Z}/\mathbb{Z}n = \widehat{G}$ with $\overline{k} \bullet \overline{l} := \overline{kl} \in \mathbb{Z}_n$ and hence $\langle \widehat{k}, \widehat{l}\rangle = \zeta^{kl} = \exp(-2\pi i \frac{kl}{n})$.

We identify

$$\begin{gathered} G = \mathbb{Z}_n = \{\overline{0}, \cdots, \overline{n-1}\} = \{0, \cdots, n-1\}, \\ \mathbb{C}^G = \mathbb{C}^{\widehat{G}} = \mathbb{C}^{\mathbb{Z}_n} = \mathbb{C}^n \ni a = (a(\overline{k}))_{\overline{k}\in\mathbb{Z}_n} \\ = (a(\overline{0}), \cdots, a(\overline{n-1}) = (a(0), \cdots, a(n-1)), \text{ and hence} \\ \mathrm{Four}_G = \mathrm{Four}_{\widehat{G}} : \mathbb{C}^n \to \mathbb{C}^n. \end{gathered}$$

The Fourier transform of $a = (a(0), \cdots, a(n-1))$ is

$$\begin{gathered} \widehat{a} = (\widehat{a}(0), \cdots, \widehat{a}(n-1)), \\ \widehat{a}(l) = \textstyle\sum_{\overline{k}\in\mathbb{Z}_n} a(k)\langle \overline{k}, \overline{l}\rangle = \sum_{k=0}^{n-1} a(k)\zeta^{kl} = \sum_{k=0}^{n-1} a(k)\exp\left(-2\pi i \frac{kl}{n}\right). \end{gathered}$$

(2) Let $d := 2$, $K := \mathbb{R}$, $\zeta := -1$, and $G = \mathbb{Z}_2^r \ni g = (g_1, \cdots, g_r)$ the finite-dimensional $\mathbb{Z}_2$-vector space which is the typical finite group of exponent 2. We choose

$$\widehat{G} := G,\ g \bullet h := g_1h_1 + \cdots + g_rh_r, \text{and hence } \langle g, h\rangle = (-1)^{g\bullet h}.$$

The *Fourier transform* $\widehat{a}$ of $a \in \mathbb{R}^G$ is given by $\widehat{a}(h) = \sum_{g\in G} a(g)(-1)^{g\bullet h}$. One also talks about the *Walsh–Fourier transform* in this case.

LEMMA 21. *For each $g \in G$ the Fourier transform of*

$$\delta_g \in K^G \text{ is } \widehat{\delta_g} = \langle g, -\rangle \in \mathrm{Gr}(\widehat{G}, \mu) \subset K^{\widehat{G}}.$$

Proof. $\widehat{\delta_g}(\widehat{g}) = \sum_{h\in G} \delta_g(h)\langle h, \widehat{g}\rangle = \langle g, \widehat{g}\rangle$. □

The K-module K^G admits two structures as commutative K-algebras which are both significant for the DFT.

LEMMA AND DEFINITION 22. *With the argumentwise multiplication*

$$(a_1a_2)(g) := a_1(g)a_2(g),\ a_1, a_2 \in K^G,\ g \in G, \tag{20}$$

the K-module K^G is a commutative K-algebra whose identity 1_{K^G} is the constant function with value 1. *The standard basis consists of complete orthogonal idempotents, i.e.,*

$$\textstyle\sum_{g\in G} \delta_g = 1,\ \delta_g\delta_h = \delta_{g,h}\delta_g.$$

The proof is obvious.

LEMMA AND DEFINITION 23. *With the* convolution *multiplication*

$$(a_1 * a_2)(g) := \sum_{g_1+g_2=g} a_1(g_1)a_2(g_2) = \sum_{h\in G} a_1(g-h)a_2(h) = \sum_{h\in G} a_1(h)a_2(g-h) \tag{21}$$

the K-module K^G is a commutative K-algebra with the identity δ_0. One writes $K[G] := (K^G, *)$ and calls this algebra the group algebra *of G with coefficients in K. The map*

$$\delta : G \to U(K[G]),\ g \mapsto \delta_g, \tag{22}$$

is a group monomorphism, i.e., injective with

$$\delta_0 = 1,\ \delta_{g_1+g_2} = \delta_{g_1} * \delta_{g_2},\ \text{hence } \delta_g^{-1} = \delta_{-g}.$$

The proof is analogous to that for the polynomial algebra $K[X] := K[\mathbb{N}]$ and is omitted.

The map $\delta : G \to U(K[G])$ has the following *universal property*. For two K-algebras A and B let $\mathrm{Al}_K(A, B)$ denote the set of K-algebra homomorphisms from A to B.

THEOREM 24 (universal property). *For each K-algebra B the map*

$$\mathrm{Al}_K(K[G], B) \to \mathrm{Gr}(G, \mathrm{U}(B)),\ \varphi \mapsto \chi := \varphi \circ \delta, \tag{23}$$

is bijective. The inverse map is given by

$$\chi \mapsto \varphi,\ \varphi(a) = \sum_{g\in G} a(g)\chi(g),\ a \in K^G.$$

Proof. The map is injective since $\chi := \varphi \circ \delta,\ \chi(g) = \varphi(\delta_g)$, implies

$$\varphi(a) = \varphi\left(\sum_{g\in G} a(g)\delta_g\right) = \sum_{g\in G} a(g)\varphi(\delta_g) = \sum_{g\in G} a(g)\chi(g). \tag{24}$$

Let, conversely, χ be given and define φ via the K-linear map (24), in particular,

$$\varphi(\delta_g) = \chi(g) \text{ and } \varphi(1_{K[G]}) = \varphi(\delta_0) = \chi(0) = 1_B.$$

Then

$$\varphi(\delta_{g_1} * \delta_{g_2}) = \varphi(\delta_{g_1+g_2}) = \chi(g_1+g_2) = \chi(g_1)\chi(g_2) = \varphi(\delta_{g_1})\varphi(\delta_{g_2}).$$

Therefore φ is multiplicative on the standard basis and therefore a K-algebra homomorphism by bilinear extension. ∎

COROLLARY 25. *For $B := K$ there results the bijection*

$$\mathrm{Al}_K(K[G], K) \cong \mathrm{Gr}(G, \mathrm{U}(K)),\ \varphi \mapsto \varphi \circ \delta.$$

In particular, for every $\widehat{g} \in \widehat{G}$, the group homomorphism $\langle -, \widehat{g}\rangle : G \to \mu \subseteq \mathrm{U}(K)$ induces the K-algebra homomorphism

$$K[G] = (K^G, *) \to K,\ a \mapsto \sum_{g\in G} a(g)\langle g, \widehat{g}\rangle = \widehat{a}(\widehat{g}).$$

THEOREM 26 (convolution theorem). *The K-linear Fourier transform* $\mathrm{Four}_G : K[G] \to K^{\widehat{G}}$ *is an algebra homomorphism, i.e.,*

$$\widehat{\delta_0} = \langle 0, -\rangle = 1_{K^{\widehat{G}}},\ \widehat{a_1 * a_2}(\widehat{g}) = \widehat{a_1}(\widehat{g})\widehat{a_2}(\widehat{g}).$$

Proof. Since $K^{\widehat{G}}$ is supplied with the argumentwise multiplication, the theorem is a direct consequence of the Corollary 25. □

COROLLARY AND DEFINITION 27 (Antipode). *The group automorphism $g \mapsto -g$ of G induces the algebra automorphism*

$$\mathrm{S}_G : K^G \cong K^G,\ \delta_g \mapsto \delta_{-g},\ \mathrm{S}_G(a)(g) = a(-g),$$

with respect to both multiplications on K^G. This map is called the antipode *on K^G and is an involution, i.e., $\mathrm{S}_G^2 = \mathrm{id}_{K^G}$ or $\mathrm{S}_G^{-1} = \mathrm{S}_G$. We likewise define $\mathrm{S}_{\widehat{G}}$ on $K^{\widehat{G}}$.*

Proof. For the convolution multiplication this follows from the universal property of $K[G]$, and for the argumentwise multiplication directly from the definition. □

LEMMA 28. *The antipode commutes with the Fourier transform, i.e., the diagram*

$$\begin{array}{ccc} K^G & \stackrel{\mathrm{Four}_G}{\longrightarrow} & K^{\widehat{G}} \\ \downarrow\ \mathrm{S}_G & & \downarrow \mathrm{S}_{\widehat{G}} \\ K^G & \stackrel{\mathrm{Four}_G}{\longrightarrow} & K^{\widehat{G}} \end{array} \quad \textit{is commmutative or } \mathrm{Four}_G \mathrm{S}_G = \mathrm{S}_{\widehat{G}} \mathrm{Four}_G\,.$$

Proof. $\mathrm{Four}_G \mathrm{S}_G(\delta_g) = \mathrm{Four}_G(\delta_{-g}) = \langle -g, - \rangle = \mathrm{S}_{\widehat{G}}(\langle g, - \rangle) = \mathrm{S}_{\widehat{G}} \mathrm{Four}_G(\delta_g)$. □

For the proof of the *Fourier inversion theorem* we need an additional assumption on the root ζ.

Assumption 29 (see [16, Satz 2.8]). For the data of Assumption 14 we assume in what follows that d is invertible in K and that for each divisor $m > 1$ of d and the root $\eta := \zeta^{\frac{d}{m}}$ of order $\mathrm{ord}(\eta) = m$ the relation

$$1 + \eta + \cdots + \eta^{m-1} = 0$$

holds. In Theorem 80 we will give several equivalent conditions for this assumption as in [16, Satz 2.8].

Recall that all considered groups G are finite abelian of exponent d ($dG = 0$). Let $N := \mathrm{ord}(G)$ denote the order of G.

COROLLARY 30. *The preceding Assumption* 29 *is satisfied if K is a field.*

Proof. The second property follows from the relation

$$0 = \eta^m - 1 = (\eta - 1)(\eta^{m-1} + \cdots + \eta + 1)$$

since $\mathrm{ord}(\eta) = m \neq 1$; hence $\eta \neq 1$. Assume that the characteristic p of K divides d or $d = 0$ in K. Then p is prime and

$$d = pk \ \Rightarrow\ 0 = \zeta^d - 1 = (\zeta^k)^p - 1^p = (\zeta^k - 1)^p \ \Rightarrow\ \zeta^k = 1 \ \Rightarrow\ \mathrm{ord}(\zeta) \leq k < d,$$

a contradiction to $\mathrm{ord}(\zeta) = d$. □

COROLLARY 31. *Under Assumption* 29 *the order $N := \mathrm{ord}(G)$ of G is also invertible in K.*

Proof. If $G \cong \mathbb{Z}/\mathbb{Z}d_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}d_r$ with $d_\varrho \mid d$, then $N = d_1 * \cdots * d_r$ divides d^r and therefore is invertible like d. □

LEMMA 32. *Under Assumption* 29 *any character $\chi \in Gr(G, \mu)$ of the group G satisfies the relation*

$$\textstyle\sum_{g \in G} \chi(g) = N\delta_{1,\chi} = \begin{cases} N & \text{if } \chi = 1, \\ 0 & \text{if } \chi \neq 1. \end{cases}$$

Here $1 : G \to \mu,\ g \mapsto 1$, *denotes the trivial character which is the neutral element of the character group.*

Proof. The assertion is obvious for $\chi = 1$. Assume therefore that $\chi \neq 1$ and that the image $\mathrm{im}(\chi)$ has the order $m \neq 1$. Then $\mathrm{im}(\chi)$ is the unique subgroup of order m of the cyclic group $\mu = \langle\zeta\rangle$ and is generated by $\eta := \zeta^{\frac{d}{m}}$; hence $\mathrm{im}(\chi) = \langle\eta\rangle = \{1, \eta, \cdots, \eta^{m-1}\}$. Let $\eta = \chi(g)$. The isomorphism

$$G/\ker(\chi) \cong \mathrm{im}(\chi) = \langle\eta\rangle, \overline{ig} \mapsto \chi(ig) = \chi(g)^i = \eta^i,$$

implies that every element $h \in G$ has a unique representation

$$h = ig + k, 0 \leq i \leq m-1, k \in \ker(\chi).$$

We infer

$$\begin{aligned}\textstyle\sum_{h\in G} \chi(h) &= \textstyle\sum \{\chi(ig+k); 0 \leq i \leq m-1, k \in \ker(\chi)\} \\ &= \textstyle\sum_{i,k} \chi(g)^i = \sum_k \left(\sum_{i=0}^{m-1} \eta^i\right) = 0,\end{aligned}$$

where $\sum_{i=0}^{m-1} \eta^i = 0$ according to Assumption 29. ∎

THEOREM 33. *The following equations hold for* $a \in K^G,\ b \in K^{\widehat{G}},\ g \in G,\ \widehat{g} \in \widehat{G}$:

$$\begin{aligned}Na(0) = \textstyle\sum_{\widehat{g}\in\widehat{G}} \widehat{a}(\widehat{g}),\ Nb(0) = \textstyle\sum_{g\in G} \widehat{b}(g), \\ N\delta_{0,g} = \textstyle\sum_{\widehat{g}\in\widehat{G}} \langle g, \widehat{g}\rangle,\ N\delta_{0,\widehat{g}} = \textstyle\sum_{g\in G} \langle g, \widehat{g}\rangle.\end{aligned}$$

Proof. Since $\widehat{\delta_g} = \langle g, -\rangle$ and $\widehat{\delta_{\widehat{g}}} = \langle -, \widehat{g}\rangle$ only the first equation has to be shown. With $\chi := \langle g, -\rangle : \widehat{G} \to \mu$ Lemma 32 implies $\sum_{\widehat{g}\in\widehat{G}} \langle g, \widehat{g}\rangle = N\delta_{0,g}$; hence

$$\begin{aligned}\textstyle\sum_{\widehat{g}\in\widehat{G}} \widehat{a}(\widehat{g}) = \textstyle\sum_{\widehat{g}\in\widehat{G}, g\in G} a(g)\langle g, \widehat{g}\rangle \\ = \textstyle\sum_g a(g) \sum_{\widehat{g}} \langle g, \widehat{g}\rangle = \sum_g a(g) N\delta_{0,g} = Na(0).\end{aligned}$$ ∎

THEOREM 34 (Fourier inversion theorem). *Under Assumption* 29 *the Fourier transform* Four_G *is an isomorphism and*

$$\begin{aligned}\mathrm{Four}_{\widehat{G}} \circ \mathrm{Four}_G = N\,\mathrm{S}_G \ \textit{or}\ \mathrm{Four}_G^{-1} = N^{-1}\,\mathrm{S}_G\,\mathrm{Four}_{\widehat{G}} = N^{-1}\,\mathrm{Four}_{\widehat{G}}\,\mathrm{S}_{\widehat{G}} \ \textit{or} \\ \widehat{\widehat{a}}(g) = Na(-g) \ \textit{or}\ \widehat{\widehat{a}} = N\,\mathrm{S}_G(a).\end{aligned}$$

Proof. All assertions follow from the last equation which has to be shown for the standard basis vectors only, from the invertibility of N and of the antipode and the same properties for $\mathrm{Four}_{\widehat{G}}$ instead of Four_G. But for $g, h \in G$

$$\begin{aligned}\widehat{\widehat{\delta_h}}(g) = \widehat{\langle h, -\rangle}(g) = \textstyle\sum_{\widehat{g}\in\widehat{G}} \langle h, \widehat{g}\rangle\langle g, \widehat{g}\rangle = \sum_{\widehat{g}\in\widehat{G}} \langle g+h, \widehat{g}\rangle \\ = N\delta_{0,g+h} = N\delta_{-h}(g) = N\,\mathrm{S}_G(\delta_h)(g);\ \text{hence}\ \widehat{\widehat{\delta_h}} = N\,\mathrm{S}_G(\delta_h).\end{aligned}$$ ∎

Example 35. In the situation of Example 20(1), with $d = N = n$ the Fourier inversion has the form

$$a \leftrightarrow \widehat{a},\ \widehat{a}(l) = \textstyle\sum_{k=0}^{n-1} a(k) \exp\left(-2\pi i \frac{kl}{n}\right),\ a(k) = n^{-1} \sum_{l=0}^{n-1} \widehat{a}(l) \exp\left(+2\pi i \frac{kl}{n}\right).$$

THEOREM 36 (product theorem). *The map* $N^{-1}\,\mathrm{Four}_G : K^G \to K[\widehat{G}]$ *is an algebra isomorphism; i.e.,*

$$N^{-1}\widehat{a_1 a_2} = N^{-1}\widehat{a_1} * N^{-1}\widehat{a_2} \ \textit{or}\ \widehat{a_1 a_2} = N^{-1}\widehat{a_1} * \widehat{a_2} \ \textit{and}\ N^{-1}\widehat{1} = \delta_0 \ \textit{or}\ \widehat{1} = N\delta_0.$$

Proof. The Fourier inversion theorem (Theorem 34) and Lemma 28 imply that $N^{-1}\,\mathrm{S}_G\,\mathrm{Four}_{\widehat{G}} : K^{\widehat{G}} \to K[G]$ and $\mathrm{S}_G : K[G] \to K[G]$ are algebra isomorphisms. The same follows for $N^{-1}\,\mathrm{Four}_{\widehat{G}}$ and then also for $N^{-1}\,\mathrm{Four}_G$. ∎

The action of the group G on itself by translation induces an action on K^G by K-algebra automorphisms, viz.,

$$\circ : G \times K^G, (g,a) \mapsto g \circ a := \delta_g * a, \quad (g \circ a)(h) = a(h-g). \tag{25}$$

Similarly $\widehat{G}$ acts on $K^{\widehat{G}}$.

THEOREM 37 (shift theorem). *For $a \in K^G$, $g \in G$, and $\widehat{g} \in \widehat{G}$ the following relations hold:*

$$\mathrm{Four}_G(g \circ a) = \langle g, - \rangle \widehat{a}, \quad \mathrm{Four}_G(\langle -, \widehat{g} \rangle a) = (-\widehat{g}) \circ \widehat{a}. \tag{26}$$

Proof. The first equation follows from the convolution theorem since

$$\widehat{g \circ a} = \widehat{\delta_g * a} = \widehat{\delta}_g \widehat{a} = \langle g, - \rangle \widehat{a},$$

and the second from

$$\begin{gathered} \mathrm{Four}_G(\langle -, \widehat{g}_1 \rangle a)(\widehat{g}_2) = \textstyle\sum_{g \in G} \langle g, \widehat{g}_1 \rangle a(g) \langle g, \widehat{g}_2 \rangle \\ = \textstyle\sum_{g \in G} a(g) \langle g, \widehat{g}_1 + \widehat{g}_2 \rangle = \widehat{a}(\widehat{g}_1 + \widehat{g}_2) = ((-\widehat{g}_1) \circ \widehat{a})(\widehat{g}_2). \end{gathered}$$ ∎

COROLLARY AND DEFINITION 38 (correlation). *The* correlation function $a \circ b \in K^G$ *of two functions $a, b \in K^G$ is defined as*

$$\begin{gathered} a \circ b := (\mathrm{S}_G\, a) * b, \ \textit{i.e.}\ , \\ (a \circ b)(h) := \textstyle\sum_{g \in G} (\mathrm{S}_G\, a)(g) b(h-g) \\ = \textstyle\sum_{g \in G} a(-g) b(h-g) = \sum_{g \in G} a(g) b(h+g). \end{gathered}$$

Then

$$b \circ a = \mathrm{S}_G(a \circ b) \ \textit{and}\ \mathrm{Four}_G(a \circ b) = (\mathrm{S}_{\widehat{G}}\, \widehat{a}) \widehat{b}.$$

Proof. Since S_G is an involution and an algebra homomorphism, we infer

$$S_G(a \circ b) = S_G^2 a * S_G b = S_G b * a = b \circ a.$$

The second equation follows from the convolution theorem and from $\mathrm{S}_{\widehat{G}}\,\mathrm{Four}_G = \mathrm{Four}_G\,\mathrm{S}_G$. ∎

For the coefficient field $K := \mathbb{C}$ the preceding considerations can be slightly changed. For a function $a \in \mathbb{C}^G$ we define the complex conjugate function $\overline{a} \in \mathbb{C}^G$ as $\overline{a}(g) := \overline{a(g)}$ and likewise for $a \in \mathbb{C}^{\widehat{G}}$. On $\mathbb{C}^G$ and likewise on $\mathbb{C}^{\widehat{G}}$ we define the standard hermitian inner product

$$(a_1, a_2) := \textstyle\sum_{g \in G} \overline{a_1(g)} a_2(g) = \sum_{g \in G} (S\overline{a_1})(-g) a_2(g) = (S\overline{a_1} * a_2)(0) = (\overline{a_1} \circ a_2)(0), \tag{27}$$

where S denotes either S_G or $S_{\widehat{G}}$.

LEMMA 39. $\widehat{\overline{a}} = \overline{S\widehat{a}}$, *and hence* $S\widehat{\overline{a}} = \overline{\widehat{a}}$.

Proof.

$$\widehat{\overline{a}}(\widehat{g}) = \textstyle\sum_g \overline{a(g)} \langle g, \widehat{g} \rangle = \overline{\sum_g a(g) \langle g, -\widehat{g} \rangle} = \overline{S\widehat{a}(\widehat{g})}.$$ ∎

THEOREM 40 (Plancherel). *For* $a_1, a_2 \in \mathbb{C}^G$: $N(a_1, a_2) = (\widehat{a_1}, \widehat{a_2})$.

Proof. Using (27), Theorem 33, Corollary 38, and finally the preceding lemma, we get

$$\begin{aligned} N(a_1, a_2) = N(\overline{a_1} \circ a_2)(0) = \textstyle\sum_{\widehat{g} \in \widehat{G}} \widehat{\overline{a_1} \circ a_2}(\widehat{g}) \\ = \textstyle\sum_{\widehat{g} \in \widehat{G}} ((S\widehat{\overline{a_1}})\widehat{a_2})(\widehat{g}) = \textstyle\sum_{\widehat{g} \in \widehat{G}} (\widehat{\overline{a_1}}\widehat{a_2})(\widehat{g}) = (\widehat{a_1}, \widehat{a_2}). \end{aligned}$$ □

COROLLARY 41 (orthogonality relations). *For two characters* $a_i := \langle -, \widehat{g_i} \rangle$, $\widehat{g_1}$, $\widehat{g_2} \in \widehat{G}$, *on* G *one obtains the orthogonality relation*

$$(a_1, a_2) = N(\delta_{\widehat{g_1}}, \delta_{\widehat{g_2}}) = N\delta_{\widehat{g_1}, \widehat{g_2}}.$$

Hence the characters $\langle -, \widehat{g} \rangle$ *are an orthogonal basis of* $\mathbb{C}^G$.

Proof. This follows from the preceding theorem and $\widehat{\delta_{\widehat{g_i}}} = \langle -, \widehat{g_i} \rangle$ with the roles of G and $\widehat{G}$ interchanged. □

4. Linear complexity. The FFT is a *fast* algorithm for the computation of the DFT. An algorithm is called fast if it has low complexity. In this section we define the *linear complexity* [9, Chap. 13] of matrices and in particular of the DFT to make this terminology precise. See [37] or the book [9] for a comprehensive treatment of *algebraic complexity theory*.

Let K again denote a commutative ring and I, J finite sets, for instance, G and $\widehat{G}$ in the preceding section. We consider the free column module $K^J := K^{J \times 1}$ with the column vectors $\xi = (\xi_j)_{j \in J}$, the free row module $K^{1 \times J}$ with the row vectors $x = (x_j)_{j \in J}$ and the standard basis δ_j, $j \in J$, and the free module $K^{I \times J}$ of $I \times J$ matrices with coefficients in K. We identify

$$\begin{aligned} K^{I \times J} &= \mathrm{Hom}_K(K^J, K^I),\ A = (\xi \mapsto A\xi),\ \text{in particular,} \\ K^{1 \times J} &= \mathrm{Hom}_K(K^J, K),\ x = (\xi \mapsto x\xi = \textstyle\sum_{j \in J} x_j \xi_j). \end{aligned} \tag{28}$$

The following considerations will be applied mainly to $\mathrm{Four}_G \in K^{\widehat{G} \times G} = \mathrm{Hom}_K(K^G, K^{\widehat{G}})$. In the complexity theoretic arguments below we will mostly assume $A \in K^{m \times n}$.

Motivation 42. For $A \in K^{I \times J}$ the complexity or cost of an algorithm for the computation of $A\xi$ for arbitrary ξ will be the number of necessary *elementary computation steps* whose cost is defined to be 1. Such a step could be an addition or a multiplication, but we will use steps of the form $(x, y) \mapsto ax + y$ of one multiplication and one addition for numbers a, x, y in K as realized in many standard computer processors. If, more generally, $a \in K$ is a constant and $v, w \in K^{1 \times J}$, $\xi \in K^J$ are vectors, then $(av + w)\xi = a(v\xi) + (w\xi)$; i.e., the result is obtained from the numbers $v\xi$ and $w\xi$ with one elementary computation step. This motivates the following definitions of an algorithm and its complexity.

DEFINITION 43. *Let* I, J *be finite sets and let* $A \in K^{I \times J}$. *A* sequential algorithm *of* complexity *or* cost $M \geq 0$ *for* A *or, in more detail, for the computation of* $A\xi$ *for all* $\xi \in K^J$ *is a sequence* $v_1, \cdots, v_M$ *of row vectors in* $K^{1 \times J}$ *with the following properties.*

1. *Each row* A_{i-}, $i \in I$, *belongs to* $V := \{\delta_j;\ j \in J\} \cup \{0\} \cup \{v_1, \cdots, v_M\}$.
2. *For each* $k = 1, \cdots, M$ *the vector* v_k *is given in the form* $v_k = av + w$, *where* $a \in K$ *and* $v, w \in \{\delta_j;\ j \in J\} \cup \{0\} \cup \{v_1, \cdots, v_{k-1}\}$.

The data a, v, w depend on k, but do not get an index for notational simplicity. The algorithm to compute $A\xi$ for arbitrary ξ computes the list of M values $v_1\xi, \cdots, v_M\xi$ with M elementary computation steps $v_k\xi = a(v\xi) + (w\xi)$ for values $v\xi$ and $w\xi$ computed earlier, and the $(A\xi)_i = A_{i-}\xi,\ i \in I$, are among these by condition (1) of Definition 43. In contrast, the computation of $0\xi = 0$ and $\delta_j\xi = \xi_j$ is costless. This signifies that the access time to the components of ξ on a real computer is neglected.

LEMMA 44. *For the computation of $A \in K^{m\times n}$ there is an algorithm of complexity $\leq mn$.*

Proof. The algorithm is the standard one for the matrix-vector product and is given by the sequence of vectors

$$\begin{array}{ccccccc}
v_{1,1} := A_{11}\delta_1 & \cdots & v_{1,j} = A_{1j}\delta_j + v_{1,j-1} & \cdots & v_{1,n} = A_{1-} = A_{1n}\delta_n + v_{1,n-1} \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
v_{i,1} := A_{i1}\delta_1 & \cdots & v_{i,j} = A_{ij}\delta_j + v_{i,j-1} & \cdots & v_{i,n} = A_{i-} = A_{in}\delta_n + v_{i,n-1} \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
v_{m,1} := A_{m1}\delta_1 & \cdots & v_{m,j} = A_{mj}\delta_j + v_{m,j-1} & \cdots & v_{m,n} = A_{m-} = A_{mn}\delta_n + v_{m,n-1}.
\end{array} \qquad \square$$

If in the preceding proof $A_{ij} = 0$ and hence $v_{i,j} = v_{i,j-1}$, one of these vectors can be omitted and hence the following corollary holds.

COROLLARY 45. *If N is the number of nonzero components of a matrix $A \in K^{m\times n}$, then there is an algorithm for A of complexity N.*

DEFINITION AND COROLLARY 46. *The* linear complexity $\mu(A)$ *of a matrix $A \in K^{I\times J}$ is the minimal complexity of an algorithm for A. Then*

(1) *$\mu(A) \leq N$, where N is the number of non-zero components of A;*
(2) *$\mu(A) = 0$ if and only if each row of A is either zero or a standard basis vector;*
(3) *$\mu(1, a_2, \cdots, a_n) \leq n - 1$ for $a_2, \cdots, a_n \in K$.*

More generally, if ${}_KW$ and ${}_KV$ are free K-modules of finite dimension, then $n := [W : K]$ (resp., $m := [V : K]$), if $\underline{w} = (w_1, \cdots, w_n)$ (resp., $\underline{v} = (v_1, \cdots, v_m)$) are fixed chosen bases of these modules, and if $f : W \to V$, $f(\underline{w}) = \underline{v}A$, is a linear map with the matrix A with respect to the chosen bases*, then we define the complexity*

$$\mu(f) := \mu_{\underline{w},\underline{v}}(f) := \mu(A)$$

as that of the matrix A. Of course, basis transformations of V do not have complexity zero in general.

Proof. Concerning the last item the $1 \times n$ matrix $A := (1, a_2, \cdots, a_n)$ admits the algorithm $v_2 := \delta_1 + a_2\delta_2, \cdots, v_n := A$ since the computation of $1\xi_1 = \xi_1$ is of complexity zero. $\square$

COROLLARY 47. *If Assumption* 29 *holds and G is a group of order N, the complexity of the Fourier transform* $\mathrm{Four}_G = (\langle g, \widehat{g}\rangle)_{\widehat{g}\in\widehat{G}, g\in G} \in K^{\widehat{G}\times G}$ *is at most $N(N-1)$.*

Proof. This follows like item 3 of Corollary 46 since for the column index $g := 0$ and any row index $\widehat{g}$ the entry of Four_G is $\langle 0, \widehat{g}\rangle = 1$. $\square$

DEFINITION AND COROLLARY 48. *If $\alpha : I \to J$ is any map between finite index sets, the map*

$$K^\alpha : K^J \to K^I,\ \xi = (\xi_j)_{j\in J} \mapsto \xi \circ \alpha = (\xi_{\alpha(i)})_{i\in I}$$

is called an index transformation *and is of complexity zero.*

Proof. The computation of $K^\alpha(\xi)_i = \xi_{\alpha(i)}$ just reads off one component of ξ, and these operations are costless. $\square$

The following theorem is decisive for the computation of an upper bound of the FFT.

THEOREM 49. *If $A \in K^{m\times n}$ and $B \in K^{n\times p}$, then $\mu(AB) \leq \mu(A) + \mu(B)$.*

Proof. Let $v_1, \cdots, v_M$ (resp., $w_1, \cdots, w_N$ be algorithms for A resp., B of minimal complexity $M := \mu(A)$ and $N := \mu(B)$. We are going to show that $w_1, \cdots, w_N, v_1B, \cdots, v_MB$ is an algorithm for AB; hence $\mu(AB) \leq M + N = \mu(A) + \mu(B)$. Let

$$\begin{aligned} V_A &:= \{\delta_i;\ i = 1, \ldots, n\} \cup \{0\} \cup \{v_1, \cdots, v_M\}, \\ V_B &:= \{\delta_j;\ j = 1, \ldots, p\} \cup \{0\} \cup \{w_1, \cdots, w_N\}, \\ V_{AB} &:= \{\delta_j;\ j = 1, \ldots, p\} \cup \{0\} \cup \{w_1, \cdots, w_N, v_1B, \cdots, v_MB\}. \end{aligned}$$

By definition $V_B \subseteq V_{AB}$. We have to show that V_{AB} satisfies properties (1) and (2) from Definition 43.

(1) We use $A_{i-} \in V_A,\ B_{j-} \in V_B$ and show that $(AB)_{i-} = A_{i-}B \in V_{AB}$.

Case 1. $A_{i-} = 0 \ \Rightarrow\ A_{i-}B = 0 \in V_{AB}$.

Case 2. $A_{i-} = \delta_k \ \Rightarrow\ A_{i-}B = \delta_kB = B_{k-} \in V_B \subseteq V_{AB}$.

Case 3. $A_{i-} = v_k \ \Rightarrow\ A_{i-}B = v_kB \in V_{AB}$.

(2) We have to show that each vector x in $\{w_1, \cdots, v_MB\}$ is obtained from vectors in V_{AB} preceding x by an elementary computation step. For the vectors $w_l \in V_B$ this is obvious. Therefore consider a vector $x = v_kB \in V_{AB}$, where $v_k = au_1 + u_2$ with $a \in K$ and vectors $u_1, u_2 \in V_A$ preceding v_k. Then $x = v_kB = a(u_1B) + (u_2B)$, and we have to show that u_1B and u_2B precede x in V_{AB}.

Case 1. $u_j = 0 \ \Rightarrow\ u_jB = 0 \in V_{AB}$ preceding x.

Case 2. $u_j =$ standard basis vector $\ \Rightarrow\ u_jB =$ row of $B \ \Rightarrow\ u_jB \in V_B \subseteq V_{AB}$ preceding $x = v_kB$.

Case 3. $u_j = v_l,\ l < k \ \Rightarrow\ u_jB = v_lB \in V_{AB}$ preceding $x = v_kB$.

Hence V_{AB} has the properties of an algorithm. □

COROLLARY 50. *The complexity of block matrices satisfies*

$$\mu\left(\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}\right) \leq \mu(A) + \mu(B),\ A, B \in K^{\bullet\times\bullet} \text{ of arbitrary size.}$$

Proof. Theorem 49, $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right) = \left(\begin{smallmatrix} A & 0 \\ 0 & \mathrm{id} \end{smallmatrix}\right)\left(\begin{smallmatrix} \mathrm{id} & 0 \\ 0 & B \end{smallmatrix}\right)$, and the trivial relation $\mu\left(\begin{smallmatrix} A & 0 \\ 0 & \mathrm{id} \end{smallmatrix}\right) = \mu(A)$ yield the result. □

Remark 51 (multiplicative complexity). Let $(X - x_1) * \cdots * (X - x_n) \in \mathbb{Q}[X] \subset \mathbb{C}[X]$ be a rational polynomial with n distinct rational roots $x_i,\ i = 1, \ldots, n$. Then Lagrange interpolation or the Chinese remainder theorem implies the canonical $\mathbb{C}$-isomorphism

$$\varphi : \mathbb{C}[X]_{<n} \cong \mathbb{C}^n,\ f \mapsto (f(x_1), \cdots, f(x_n)),$$

where $\mathbb{C}[X]_{\langle n}$ is the space of polynomials of degree less than n. The domain (resp., the codomain) of φ has the basis $1, \cdots, X^{n-1}$ (resp., the standard basis $\delta_1, \cdots, \delta_n$). For fixed j and $f = a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$ euclidean division furnishes

$$\begin{gathered} f = g(X - x_j) + f(x_j),\ g := b_{n-2}X^{n-2} + \cdots + b_0 \text{ with} \\ b_{n-2} = a_{n-1},\ b_{i-1} = a_i + x_jb_i,\ i = n-2, \ldots, 1,\ f(x_j) = a_0 + x_jb_0. \end{gathered}$$

This shows that $f(x_j)$ can be computed from f with $n - 1$ elementary computation steps and hence $\mu(\varphi) \leq n(n-1)$. Observe, however, that the necessary multiplications have the rational factor x_j. In the multiplicative complexity theory due to Winograd

[43] which is, for instance, also used in [29] or [20], these rational multiplications—at least if the x_j are small integers—and rational linear combinations are considered costless, and therefore the complexity of φ is considered to be zero. This is not justified for those computers where the elementary computation step consists of one multiplication and one addition. The same cautionary remarks apply to almost all fast algorithms which use the Chinese remainder theorem and which are not discussed in this paper.

5. The fast Fourier transform (FFT). This is the central section of this article. Assumptions 14 and 29 are in force, all groups are finite abelian of exponent $d > 0$.

Reminder 52. If $\varphi : G \to H$ is a group epimorphism of additive groups, a map $\sigma : H \to G$ is called a *section* of φ if $\varphi\sigma = \mathrm{id}_H$. Then σ is injective, and the elements $\sigma(h)$, $h \in H$, are a system of representatives of $G/\ker(\varphi)$; i.e., the map

$$H \times \ker(\varphi) \to G,\ (h,k) \mapsto \sigma(h) + k, \tag{29}$$

is bijective. The map (29) is an isomorphism, and especially $G = \sigma(H) \oplus \ker(\varphi)$ if and only if σ is a monomorphism, but, in general, these properties do *not* hold.

We construct the FFT algorithm by means of a given *filtration* or sequence of subgroups

$$G_0 = 0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G. \tag{30}$$

A filtration (30) gives rise to the commutative exact diagrams (with exact rows and columns) for $i = 1, \ldots, r$:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & & & G_i/G_{i-1} & & \\
 & & \downarrow & & & & \downarrow{\scriptstyle \gamma_i:=\mathrm{inj}} & & \\
0 & \longrightarrow & G_{i-1} & \xrightarrow{\alpha_{i-1}:=\mathrm{inj}} & G & \xrightarrow{\lambda_{i-1}:=\mathrm{can}} & G/G_{i-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta_i:=\mathrm{inj}} & & \| & & \downarrow{\scriptstyle \nu_i:=\mathrm{can}} & & \\
0 & \longrightarrow & G_i & \xrightarrow{\alpha_i:=\mathrm{inj}} & G & \xrightarrow{\lambda_i:=\mathrm{can}} & G/G_i & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mu_i:=\mathrm{can}} & & & & \downarrow & & \\
 & & G_i/G_{i-1} & & & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array} \tag{31}$$

where inj (resp., can) are the canonical injections (resp., surjections). Moreover, λ_0 and α_r are isomorphisms, and the compatibility relations $\lambda_{i-1}\alpha_i = \gamma_i\mu_i$ hold. For more flexibility we now make the following, formally more general assumption.

Assumption 53. Assume that Assumptions 14 and 29 are satisfied and that

commutative exact diagrams (32) are given for $i = 1, \dots, r$:

$$
\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & & & K_i & & \\
 & & \downarrow & & & & \downarrow{\scriptstyle \gamma_i} & & \\
0 & \longrightarrow & G_{i-1} & \xrightarrow{\alpha_{i-1}} & G & \xrightarrow{\lambda_{i-1}} & H_{i-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta_i} & & \| & & \downarrow{\scriptstyle \nu_i} & & \\
0 & \longrightarrow & G_i & \xrightarrow{\alpha_i} & G & \xrightarrow{\lambda_i} & H_i & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mu_i} & & & & \downarrow & & \\
 & & K_i & & & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}
\tag{32}
$$

such that the following additional properties hold:

(1) G_0 and H_r are zero or λ_0 and α_r are isomorphisms.

(2) The compatibility relations $\lambda_{i-1}\alpha_i = \gamma_i\mu_i, i = 1, \dots, r$, hold.

(3) Sections $\sigma_i : K_i \to G_i,\ i = 1, \dots, r$, with $\mu_i\sigma_i = \mathrm{id}_{K_i}$ and $\sigma_i(0) = 0$ are chosen arbitrarily.

These diagrams, in turn, induce the filtration $0 \subseteq \alpha_1(G_1) \subseteq \cdots \subseteq \alpha_r(G_r) = G$ and the isomorphisms

$$
\begin{gathered}
G/\alpha_i(G_i) \cong H_i, \bar{g} \mapsto \lambda_i(g), \\
G_i/\beta_i(G_{i-1}) \cong \alpha_i(G_i)/\alpha_{i-1}(G_{i-1}) \cong K_i, \overline{g_i} \mapsto \overline{\alpha_i(g_i)} \mapsto \mu_i(g_i).
\end{gathered}
$$

In the situation of the preceding assumption we define

$$
N := \mathrm{ord}(G) \text{ and } e_\varrho := \mathrm{ord}(K_\varrho);\ \text{hence } N = e_1 * \cdots * e_r. \tag{33}
$$

Recall that every group admits a Jordan–Hölder series, i.e., a filtration (30) or diagrams (31) or (32) with the property that the factors $K_\varrho \cong G_\varrho/G_{\varrho-1}$ are simple or have prime order e_ϱ, and that these prime numbers are uniquely determined by G.

Application of the duality functor $G \mapsto \widehat{G}$ to the preceding diagram yields further commutative exact diagrams.

Corollary 54. *Under Assumption* 53 *the following diagrams are commutative*

and exact:

$$
\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & & & \widehat{K_j} & & \\
 & & \downarrow & & & & \downarrow{\scriptstyle \mu_j^\star} & & \\
0 & \longrightarrow & \widehat{H_j} & \xrightarrow{\lambda_j^\star} & \widehat{G} & \xrightarrow{\alpha_j^\star} & \widehat{G_j} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \nu_j^\star} & & \| & & \downarrow{\scriptstyle \beta_j^\star} & & \\
0 & \longrightarrow & \widehat{H_{j-1}} & \xrightarrow{\lambda_{j-1}^\star} & \widehat{G} & \xrightarrow{\alpha_{j-1}^\star} & \widehat{G_{j-1}} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \gamma_j^\star} & & & & \downarrow & & \\
 & & \widehat{K_j} & & & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}
\tag{34}
$$

for $j = r, r-1, \ldots, 1$. Furthermore, they have the additional properties that

1. *$\lambda_0^\star$ and $\alpha_r^\star$ are isomorphisms,*
2. *$\alpha_j^\star \lambda_{j-1}^\star = \mu_j^\star \gamma_j^\star$, and*
3. *sections $\widehat{\sigma}_j : \widehat{K_j} \to \widehat{H_{j-1}}$ with $\gamma_j^\star \widehat{\sigma}_j = \mathrm{id}_{\widehat{K_j}}$ and $\widehat{\sigma}_j(0) = 0$ are chosen arbitrarily.*

Thus, up to the reverse numbering, the diagrams from (34) satisfy the same properties as the diagrams (32) of Assumption 53, and the same arguments apply to both of them.

LEMMA 55. *Under Assumption* 53 *the map*

$$\mathrm{ind} : \textstyle\prod_{i=1}^r K_i \to G,\ k = (k_i)_{i=1,\ldots,r} \mapsto \mathrm{ind}(k) := \sum_{i=1}^r \alpha_i \sigma_i(k_i),$$

is bijective; i.e., every $g \in G$ admits a unique representation $g = \sum_{i=1}^r \alpha_i \sigma_i(k_i)$ with $k_i \in K_i$.

Proof. By induction on $i = 0, \ldots, r$ we show that $g = \alpha_i(g_i) \in \alpha_i(G_i), g_i \in G_i$, admits a unique representation

$$g = \textstyle\sum_{j=0}^i \alpha_j \sigma_j(k_j), k_j \in K_j.$$

The assertion is trivial for $i = 0$ and $\alpha_0(G_0) = 0$. For $i > 0$ the exact sequence

$$0 \to G_{i-1} \xrightarrow{\beta_i} G_i \underset{\sigma_i}{\overset{\mu_i}{\rightleftarrows}} K_i \to 0$$

with the section σ_i of μ_i and (29) imply the unique representation

$$g_i = \beta_i(g_{i-1}) + \sigma_i(k_i), g_{i-1} \in G_{i-1}, k_i \in K_i,$$

and

$$g = \alpha_i(g_i) = \alpha_i\beta_i(g_{i-1}) + \alpha_i\sigma_i(k_i) = \alpha_{i-1}(g_{i-1}) + \alpha_i\sigma_i(k_i).$$

By induction there are unique $k_j \in K_j,\ j = 0, \dots, i-1$ with

$$\alpha_{i-1}(g_{i-1}) = \textstyle\sum_{j=0}^{i-1} \alpha_j\sigma_j(k_j);\ \text{hence } g = \alpha_i(g_i) = \sum_{j=0}^{i} \alpha_j\sigma_j(k_j). \qquad \square$$

Application of the Lemma 55 to diagram (34) yields the corollary.

COROLLARY 56. *Under Assumption* 53 *every* $\widehat{g} \in \widehat{G}$ *has a unique representation*

$$\widehat{g} = \textstyle\sum_{j=1}^{r} \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j), \widehat{k}_j \in \widehat{K_j},$$

or, in other terms, the map

$$\widehat{\mathrm{ind}} : \textstyle\prod_{j=1}^{r} \widehat{K_j} \to \widehat{G}, \widehat{k} = (\widehat{k}_j)_{j=1,\dots,r} \mapsto \widehat{\mathrm{ind}}(\widehat{k}) := \sum_{j=1}^{r} \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j),$$

is bijective.

COROLLARY AND DEFINITION 57 (index transformations). *The maps*

$$\begin{gathered}\mathrm{Ind} := K^{\mathrm{ind}} : K^G \to K^{\prod_{i=1}^{r} K_i}, a \mapsto a_0 := a \circ \mathrm{ind}, \\ a_0(k_1, \dots, k_r) = a\left(\textstyle\sum_{i=1}^{r} \alpha_i\sigma_i(k_i)\right), k_i \in K_i,\end{gathered}$$

and

$$\begin{gathered}\widehat{\mathrm{Ind}} := K^{\widehat{\mathrm{ind}}} : K^{\widehat{G}} \to K^{\prod_{j=1}^{r} \widehat{K_j}}, b \mapsto b_r := b \circ \widehat{\mathrm{ind}}, \\ b_r(\widehat{k}_1, \dots, \widehat{k}_r) = b\left(\textstyle\sum_{j=1}^{r} \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j)\right)\end{gathered}$$

are K*-isomorphisms and* index transformations *according to Definition* 48, *and hence are of complexity zero.*

The following easy considerations are central for the fast computation of the Fourier transform $\widehat{a}$ of a function $a \in K^G$ given by $\widehat{a}(\widehat{g}) = \sum_{g\in G} a(g)\langle g, \widehat{g}\rangle$. According to Lemmas 55 and 56 we write g and $\widehat{g}$ as

$$\begin{gathered}g = \mathrm{ind}(k) = \textstyle\sum_{i=1}^{r} \alpha_i\sigma_i(k_i), k = (k_i)_{i=1,\dots,r} \in \prod_{i=1}^{r} K_i, \\ \widehat{g} = \widehat{\mathrm{ind}}(\widehat{k}) = \textstyle\sum_{j=1}^{r} \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j), \widehat{k} = (\widehat{k}_j)_{j=1,\dots,r} \in \prod_{j=1}^{r} \widehat{K_j},\end{gathered}$$

and compute the bimultiplicative form $\langle g, \widehat{g}\rangle$ as

$$\begin{gathered}\langle g, \widehat{g}\rangle = \left\langle \textstyle\sum_{i=1}^{r} \alpha_i\sigma_i(k_i), \sum_{j=1}^{r} \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j)\right\rangle = \textstyle\prod_{i,j=1}^{r} \mathrm{fact}_{ij}(k, \widehat{k}),\ \text{where} \\ \mathrm{fact}_{ij}(k, \widehat{k}) := \langle \alpha_i\sigma_i(k_i), \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j)\rangle = \langle \lambda_{j-1}\alpha_i\sigma_i(k_i), \widehat{\sigma}_j(\widehat{k}_j)\rangle.\end{gathered} \tag{35}$$

For $j > i$ the commutativity of the diagram (32) furnishes

$$\begin{gathered}\lambda_{j-1} \circ \alpha_i = \nu_{j-1} \circ \cdots \circ \nu_{i+1} \circ \lambda_i \circ \alpha_i = 0 \text{ since} \\ \lambda_i \circ \alpha_i = 0;\ \text{hence } \mathrm{fact}_{i,j}(k, \widehat{k}) = \langle 0, \widehat{\sigma}_j(\widehat{k}_j)\rangle = 1.\end{gathered}$$

For $j = i$ we use the compatibility condition (2) from Assumption 53 and infer

$$\begin{aligned}\mathrm{fact}_{ii}(k, \widehat{k}) &= \langle \lambda_{i-1}\alpha_i\sigma_i(k_i), \widehat{\sigma}_i(\widehat{k}_i)\rangle = \langle \gamma_i\mu_i\sigma_i(k_i), \widehat{\sigma}_i(\widehat{k}_i)\rangle \\ &= \langle \mu_i\sigma_i(k_i), \gamma_i^{\star}\widehat{\sigma}_i(\widehat{k}_i)\rangle = \langle k_i, \widehat{k}_i\rangle.\end{aligned}$$

Thus

$$\mathrm{fact}_{ij}(k, \widehat{k}) = \langle \alpha_i\sigma_i(k_i), \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j)\rangle = \begin{cases}\langle k_i, \widehat{k}_i\rangle & \text{if } i = j, \\ 1 & \text{if } i < j.\end{cases} \tag{36}$$

From (35) and (36) we infer

$$\begin{aligned}\langle g,\widehat{g}\rangle &= \textstyle\prod_{j\le i}\operatorname{fact}_{ij}(k,\widehat{k}) = \prod_{i=1}^{r}\prod_{j=1}^{i}\operatorname{fact}_{ij}(k,\widehat{k})\\ &= \textstyle\prod_{i=1}^{r}\varphi_i(k_i;\widehat{k}_1,\cdots,\widehat{k}_i),\ \text{where } \varphi_i : K_i\times\widehat{K_1}\times\cdots\times\widehat{K_i}\to K,\\ \varphi_i(k_i;\widehat{k}_1,\cdots,\widehat{k}_i) &:= \textstyle\prod_{j=1}^{i}\operatorname{fact}_{ij}(k,\widehat{k}) = \left\langle \alpha_i\sigma_i(k_i), \sum_{j=1}^{i}\lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j)\right\rangle.\end{aligned} \tag{37}$$

The decisive property of the functions φ_i is that they depend on the first i components $\widehat{k}_1,\cdots,\widehat{k}_i$ of $\widehat{k}$ only. In the same fashion (35) and (36) give rise to the representation

$$\begin{aligned}\langle g,\widehat{g}\rangle &= \textstyle\prod_{j=1}^{r}\prod_{i=j}^{r}\operatorname{fact}_{ij}(k,\widehat{k}) = \prod_{j=1}^{r}\widehat{\varphi}_j(k_j,\cdots,k_r;\widehat{k}_j) \qquad \text{with}\\ &\widehat{\varphi}_j : K_j\times\cdots\times K_r\times\widehat{K_j}\to K,\\ \widehat{\varphi}_j(k_j,\cdots,k_r;\widehat{k}_j) &:= \textstyle\prod_{i=j}^{r}\operatorname{fact}_{ij}(k,\widehat{k}) = \left\langle \sum_{i=j}^{r}\alpha_i\sigma_i(k_i), \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j)\right\rangle.\end{aligned} \tag{38}$$

For fixed $\widehat{g} = \widehat{\operatorname{ind}}(\widehat{k}) \in \widehat{G}$ Lemma 55 and (37) imply

$$\begin{aligned}\widehat{a}(\widehat{g}) &= \textstyle\sum_{g\in G}a(g)\langle g,\widehat{g}\rangle = \sum_{k\in\prod_{i=1}^{r}K_i}a(\operatorname{ind}(k))\langle\operatorname{ind}(k),\widehat{\operatorname{ind}}(\widehat{k})\rangle\\ &= \textstyle\sum_{k_1\in K_1,\cdots,k_r\in K_r}a_0(k_1,\cdots,k_r)\prod_{i=1}^{r}\varphi_i(k_i;\widehat{k}_1,\cdots,\widehat{k}_i),\end{aligned} \tag{39}$$

where $a_0 = a\circ\operatorname{ind} = \operatorname{Ind}(a)$ according to Corollary 57. This formula for $\widehat{a}(\widehat{g})$ suggests that we define, for $\varrho = 1,\dots,r$, intermediate functions

$$\begin{aligned}&a_\varrho : \widehat{K_1}\times\cdots\times\widehat{K_\varrho}\times K_{\varrho+1}\times\cdots\times K_r\to K,\\ &a_\varrho(\widehat{k}_1,\cdots,\widehat{k}_\varrho,k_{\varrho+1},\cdots,k_r)\\ &:= \textstyle\sum_{k_1\in K_1,\cdots,k_\varrho\in K_\varrho}a_0(k_1,\cdots,k_r)\prod_{i=1}^{\varrho}\varphi_i(k_i;\widehat{k}_1,\cdots,\widehat{k}_i).\end{aligned} \tag{40}$$

By definition resp. (39)

$$a_0(k_1,\cdots,k_r) = a(\operatorname{ind}(k)) \text{ and } a_r(\widehat{k}_1,\cdots,\widehat{k}_r) = \widehat{a}(\widehat{\operatorname{ind}}(\widehat{k})).$$

The next theorem is the most important result of this paper. Its main idea, viz., the recursive computation of the DFT, is due to Cooley and Tukey [18] who developed the algorithm for the group $G = \mathbb{Z}/\mathbb{Z}2^r$ on the basis of the filtration

$$G_0 := 0 \subset G_1 := \mathbb{Z}2^{r-1}/\mathbb{Z}2^r \subset\cdots\subset G_i := \mathbb{Z}2^{r-i}/\mathbb{Z}2^r \subset\cdots\subset G_r = G.$$

Later it turned out that the same idea had been used before, in particular, by Gauss. See the introduction of [8] for a short historical survey. The "decimation in time" and "decimation in frequency" terminology used below comes from the application of the DFT to the computation of one-dimensional Fourier integrals or series where $\mathbb{R}$ or $\mathbb{Z}$ are interpreted as time or frequency models, and has been adapted from [8, pp. 188–191].

THEOREM 58 (Cooley–Tukey FFT or decimation in time). *The following recursive algorithm computes the Fourier transform $\widehat{a}\in K^{\widehat{G}}$ of a function $a\in K^G$. By induction on $\varrho = 0,\cdots,r$ define functions*

$$\begin{aligned}&a_\varrho : \widehat{K_1}\times\cdots\times\widehat{K_\varrho}\times K_{\varrho+1}\times\cdots\times K_r\to K \qquad \textit{by}\\ &a_0(k_1,\cdots,k_r) := a\left(\textstyle\sum_{i=1}^{r}\alpha_i\sigma_i(k_i)\right) \ \textit{and for } 1\le\varrho\le r\\ &a_\varrho(\widehat{k}_1,\cdots,\widehat{k}_\varrho,k_{\varrho+1},\cdots,k_r)\\ &:= \textstyle\sum_{k_\varrho\in K_\varrho}a_{\varrho-1}(\widehat{k}_1,\cdots,\widehat{k}_{\varrho-1},k_\varrho,k_{\varrho+1},\cdots,k_r)\varphi_\varrho(k_\varrho;\widehat{k}_1,\cdots,\widehat{k}_\varrho), \qquad \textit{where}\\ &\varphi_\varrho(k_\varrho;\widehat{k}_1,\cdots,\widehat{k}_\varrho) = \left\langle\alpha_\varrho\sigma_\varrho(k_\varrho), \textstyle\sum_{j=1}^{\varrho}\lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j)\right\rangle.\end{aligned}$$

Then

$$\widehat{a}(\widehat{g}) = a_r(\widehat{k}_1, \cdots, \widehat{k}_r) \text{ for } \widehat{g} = \widehat{\mathrm{ind}}(\widehat{k}) = \textstyle\sum_{j=1}^{r} \lambda_{j-1}^{\star} \widehat{\sigma}_j(\widehat{k}_j) \in \widehat{G}, \widehat{k}_j \in \widehat{K_j}.$$

Proof. It remains to show that the functions a_ϱ defined in (40) satisfy these recursive relations. But for $\varrho > 0$

$$\begin{aligned} &a_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r) \\ &= \textstyle\sum_{k_1, \cdots, k_\varrho} a_0(k_1, \cdots, k_r) \prod_{i=1}^{\varrho} \varphi_i(k_i; \widehat{k}_1, \cdots, \widehat{k}_i) \\ &= \textstyle\sum_{k_\varrho \in K_\varrho} \varphi_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_\varrho) \sum_{k_1, \cdots, k_{\varrho-1}} a_0(k_1, \cdots, k_r) \prod_{i=1}^{\varrho-1} \varphi_i(k_i; \widehat{k}_1, \cdots, \widehat{k}_i) \\ &= \textstyle\sum_{k_\varrho \in K_\varrho} \varphi_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_\varrho) a_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r). \qquad \square \end{aligned}$$

The induction formula of the preceding theorem can be given another traditional form. From the definition of φ_ϱ in (37) and from (36) we infer

$$\begin{aligned} \varphi_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_\varrho) &= \left\langle \alpha_\varrho \sigma_\varrho(k_\varrho), \textstyle\sum_{j=1}^{\varrho} \lambda_{j-1}^{\star} \widehat{\sigma}_j(\widehat{k}_j) \right\rangle \\ &= \langle k_\varrho, \widehat{k}_\varrho \rangle \left\langle \alpha_\varrho \sigma_\varrho(k_\varrho), \textstyle\sum_{j=1}^{\varrho-1} \lambda_{j-1}^{\star} \widehat{\sigma}_j(\widehat{k}_j) \right\rangle \end{aligned}$$

or

$$\begin{aligned} &\varphi_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_\varrho) = \langle k_\varrho, \widehat{k}_\varrho \rangle \tau_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}) \text{ with} \\ &\tau_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}) := \left\langle \alpha_\varrho \sigma_\varrho(k_\varrho), \textstyle\sum_{j=1}^{\varrho-1} \lambda_{j-1}^{\star} \widehat{\sigma}_j(\widehat{k}_j) \right\rangle. \end{aligned} \tag{41}$$

The elements τ_ϱ are roots of unity and hence nonzero and are usually called the *twiddle factors* [8, p. 191], [5, p. 121]. With their help we define, for $\varrho = 1, \ldots, r$, the isomorphisms

$$\begin{aligned} &T_\varrho : K^{\widehat{K_1} \times \cdots \times \widehat{K_{\varrho-1}} \times K_\varrho \times \cdots \times K_r} \to K^{\widehat{K_1} \times \cdots \times \widehat{K_\varrho} \times K_{\varrho+1} \times \cdots \times K_r}, \\ &T_\varrho(c)(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r) \\ &:= \textstyle\sum_{k_\varrho \in K_\varrho} c(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r) \varphi_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_\varrho) \\ &= \mathrm{Four}_{K_\varrho}[c(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, -, k_{\varrho+1}, \cdots, k_r) \tau_\varrho(-; \widehat{k}_1, \cdots, \widehat{k}_{\varrho-1})](\widehat{k}_\varrho). \end{aligned} \tag{42}$$

Here the argument of $\mathrm{Four}_{K_\varrho}$ is a function in K^{K_ϱ} which depends on the parameters $\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_{\varrho+1}, \cdots, k_r$. The map T_ϱ is an isomorphism since the multiplication with τ_ϱ and the Fourier transform $\mathrm{Four}_{K_\varrho}$ are bijective.

THEOREM 59. *In the situation of Theorem* 58 *the induction formula computing a_ϱ from $a_{\varrho-1}$ can be expressed as $a_\varrho = T_\varrho(a_{\varrho-1})$, $\varrho = 1, \ldots, r$; hence*

$$\mathrm{Four}_G = \widehat{\mathrm{Ind}}^{-1} \circ T_r \circ \cdots \circ T_1 \circ \mathrm{Ind} : K^G \to K^{\widehat{G}}.$$

With $e_\varrho := \mathrm{ord}(K_\varrho)$ and $N := e_1 * \cdots * e_r = \mathrm{ord}(G)$ the complexity satisfies

$$\mu(\mathrm{Four}_G) \leq N(e_1 + \cdots + e_r - r).$$

Proof. The first assertion is obvious. Concerning the complexity recall the condition $\sigma_\varrho(0) = 0$ from Assumption 53 and

$$\varphi_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_\varrho) = \left\langle \alpha_\varrho \sigma_\varrho(k_\varrho), \textstyle\sum_{j=1}^{\varrho} \lambda_{j-1}^{\star} \widehat{\sigma}_j(\widehat{k}_j) \right\rangle; \text{ hence } \varphi_\varrho(0; \widehat{k}_1, \cdots, \widehat{k}_\varrho) = 1.$$

From this and equation (42) we infer $\mu(T_\varrho) \le N(e_\varrho - 1)$ as in Definition and 46(3). Since index transformations are costless according to Definition and 48, we conclude by means of Theorem 49 that

$$\mu(\mathrm{Four}_G) \le \textstyle\sum_\varrho \mu(T_\varrho) \le N(e_1 - 1 + \cdots + e_r - 1) = N(e_1 + \cdots + e_r - r). \qquad \square$$

Remark 60 (butterfly diagrams). In the literature special cases of the induction formula of Theorem 58 are often represented by means of a directed graph or so-called butterfly diagram. Such a graph can be introduced in general; it is, however, useless for the actual execution of the fast algorithm. Its graphical representation in the plane is also of no practical significance and, moreover, is complicated except in the simplest cases such as $G = \mathbb{Z}/\mathbb{Z}8$ where it is usually shown. Indeed, consider the graph $\Gamma := (V, E)$ with vertex (resp., edge) sets V(resp., E), where

$$V := \biguplus_{\varrho=0}^{r} V_\varrho, V_\varrho := \widehat{K_1} \times \cdots \times \widehat{K_\varrho} \times K_{\varrho+1} \times \cdots \times K_r,\ E \subset V \times V,$$

with edges from $(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r)$ to $(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r)$ or from $V_{\varrho-1}$ to V_ϱ only. For $w = (\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r) \in V_\varrho$, $\varrho \ge 1$, there results the bijection

$$K_\varrho \cong \{(v, w); (v, w) \text{ is an edge of } \Gamma \text{ with endpoint } w\},$$
$$k_\varrho \mapsto (v, w), v := (\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r) \in V_{\varrho-1}.$$

With the abbreviation $a(v) := a_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r)$ the recursion formula of Theorem 58 has the form

$$a(w) = \textstyle\sum a(v)\varphi_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_\varrho),$$

where $v = (\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r)$ runs over all sources of edges with sink w.

The next theorem on the "decimation in frequency" FFT computes $\mathrm{Four}_{\widehat{G}} : K^{\widehat{G}} \to K^G$ and is proved in the same fashion as Theorem 58 on the basis of (38) instead of (37). For the choice $\widehat{G} = G$ it yields a second fast algorithm for the computation of Four_G (compare [8, p. 192]).

THEOREM 61 (Sande–Tukey FFT or decimation in frequency). *Data from Assumption* 53 *and Corollary* 54. *The following algorithm computes the Fourier transform* $\widehat{b} \in K^G$ *of a function* $b \in K^{\widehat{G}}$. *By recursion from* $\varrho = r$ *to* 0 *define functions*

$$b_\varrho : \widehat{K_1} \times \cdots \times \widehat{K_\varrho} \times K_{\varrho+1} \times \cdots \times K_r \to K, \varrho = r, \ldots, 0,$$
$$b_r(\widehat{k}_1, \cdots, \widehat{k}_r) := b\left(\textstyle\sum_{j=1}^r \lambda_{j-1}^\star \widehat{\sigma}_j(\widehat{k}_j)\right), \widehat{k}_j \in \widehat{K}_j, \text{ and for } r \ge \varrho > 0$$
$$b_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r)$$
$$:= \textstyle\sum_{\widehat{k}_\varrho \in \widehat{K}_\varrho} b_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r)\widehat{\varphi}_\varrho(k_\varrho, \cdots, k_r; \widehat{k}_\varrho).$$

Then

$$\widehat{b}(g) = \textstyle\sum_{\widehat{g} \in \widehat{G}} b(\widehat{g})\langle g, \widehat{g}\rangle = b_0(k_1, \cdots, k_r) \text{ for } g = \sum_{i=1}^r \alpha_i \sigma_i(k_i) \in G, k_i \in K_i.$$

Proof. According to (38) we have

$$\widehat{b}(g) = \textstyle\sum_{\widehat{k} \in \prod_{j=1}^r \widehat{K_j}} b(\widehat{\mathrm{ind}}(\widehat{k}))\langle \mathrm{ind}\, k, \widehat{\mathrm{ind}}(\widehat{k})\rangle$$
$$= \textstyle\sum_{\widehat{k}_1 \in \widehat{K_1}, \cdots, \widehat{k}_r \in \widehat{K_r}} b_r(\widehat{k}_1, \cdots, \widehat{k}_r) \prod_{j=1}^r \widehat{\varphi}_j(k_j, \cdots, k_r; \widehat{k}_j).$$

In analogy to (40) we define functions $b_\varrho, r \geq \varrho \geq 0$, by

$$\begin{gathered} b_r(\widehat{k}_1, \cdots, \widehat{k}_r) := b(\widehat{\mathrm{ind}}(\widehat{k})) \text{ and for } \varrho < r \\ b_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r) \\ = \sum_{\widehat{k}_{\varrho+1} \in \widehat{K}_{\varrho+1}, \cdots, \widehat{k}_r \in \widehat{K}_r} b_r(\widehat{k}_1, \cdots, \widehat{k}_r) \prod_{j=\varrho+1}^r \widehat{\varphi}_j(k_j, \cdots, k_r; \widehat{k}_j) \end{gathered}$$

and show that they satisfy the recursive relations from which the theorem follows directly. But, indeed,

$$\begin{gathered} b_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r) \\ = \sum_{\widehat{k}_\varrho \in \widehat{K}_\varrho} \widehat{\varphi}_\varrho(k_\varrho, \cdots, k_r; \widehat{k}_\varrho) \sum_{\widehat{k}_{\varrho+1} \in \widehat{K}_{\varrho+1}, \cdots, \widehat{k}_r \in \widehat{K}_r} b_r(\widehat{k}_1, \cdots, \widehat{k}_r), \\ \prod_{j=\varrho+1}^r \widehat{\varphi}_j(k_j, \cdots, k_r; \widehat{k}_j) \\ = \sum_{\widehat{k}_\varrho \in \widehat{K}_\varrho} \widehat{\varphi}_\varrho(k_\varrho, \cdots, k_r; \widehat{k}_\varrho) b_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r). \qquad \square \end{gathered}$$

In analogy to (41) and (42) we also obtain, for $\varrho = r, \ldots, 1$,

$$\begin{gathered} \widehat{\varphi}_\varrho(k_\varrho, \cdots, k_r; \widehat{k}_\varrho) = \langle k_\varrho, \widehat{k}_\varrho \rangle \widehat{\tau}_\varrho(k_{\varrho+1}, \cdots, k_r; \widehat{k}_\varrho), \\ \widehat{\tau}_\varrho(k_{\varrho+1}, \cdots, k_r; \widehat{k}_\varrho) := \left\langle \sum_{i=\varrho+1}^r \alpha_i \sigma_i(k_i), \lambda_{\varrho-1}^\star \widehat{\sigma}_\varrho(\widehat{k}_\varrho) \right\rangle, \end{gathered} \tag{43}$$

and define the isomorphism

$$\begin{gathered} \widehat{T}_\varrho : K^{\widehat{K_1} \times \cdots \times \widehat{K_\varrho} \times K_{\varrho+1} \times \cdots \times K_r} \cong K^{\widehat{K_1} \times \cdots \times \widehat{K_{\varrho-1}} \times K_\varrho \times \cdots \times K_r}, \\ \widehat{T}_\varrho(c) := \mathrm{Four}_{\widehat{K_\varrho}}[c(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, -, k_{\varrho+1}, \cdots, k_r) \widehat{\tau}_\varrho(k_{\varrho+1}, \cdots, k_r; -)]. \end{gathered} \tag{44}$$

THEOREM 62. *In the situation of Theorem* 61 *and with the isomorphisms* $\widehat{T}_\varrho$ *from* (44) *and* $\mathrm{Ind}, \widehat{\mathrm{Ind}}$ *from Corollary* 57*, we have*

$$\begin{gathered} \mathrm{Four}_{\widehat{G}} = \mathrm{Ind}^{-1} \circ \widehat{T}_1 \circ \cdots \circ \widehat{T}_r \circ \widehat{\mathrm{Ind}} \text{ and} \\ \mu(\mathrm{Four}_{\widehat{G}}) \leq N(e_1 + \cdots + e_r - r), \end{gathered}$$

where $e_\varrho := \mathrm{ord}(K_\varrho)$ *and* $N := e_1 * \cdots * e_r = \mathrm{ord}(G)$.

Theorems 59 and 62 signify that the FFT-algorithms in Theorems 58 and 61 are *fast*, i.e., of relatively *low complexity* $N(e_1 + \cdots + e_r - r)$ instead of the $N(N-1)$ of the direct computation of Four_G. Recall that the algorithms and their complexity depend on the diagrams from Assumption 53.

The best FFT-algorithms according to the preceding theorems are obtained when the diagrams from Assumption 53 are constructed by means of a Jordan–Hölder series of G which are characterized by the property that the numbers e_ϱ are prime numbers; hence $N = e_1 * \cdots * e_r$ is the prime factor decomposition of $N = \mathrm{ord}(G)$.

For the next theorem we introduce a logarithm type arithmetic function Λ. Let $\mathbb{N} := \{0, 1, \cdots\}$ denote the additive monoid of natural numbers and $\mathbb{N}_{>0} := \{1, 2, \cdots\}$ the multiplicative monoid of positive numbers. Every $N \in \mathbb{N}_{>0}$ admits the unique prime factor decomposition

$$N = \prod_{p \in \mathcal{P}} p^{\mathrm{ord}_p(N)}, \ \mathrm{ord}_p(N) = 0 \text{ for almost all } p,$$

where $\mathcal{P} = \{2, 3, 5, \cdots\}$ is the set of prime numbers. The standard isomorphism

$$\mathbb{N}_{>0} \cong \mathbb{N}^{(\mathcal{P})} := \{\nu \in \mathbb{N}^{\mathcal{P}}; \nu(p) = 0 \text{ for almost all } p \in \mathcal{P}\}, N \mapsto (\mathrm{ord}_p(N))_{p \in \mathcal{P}},$$

follows and induces the composed epimorphism

$$\Lambda : \mathbb{N}_{>0} \cong \mathbb{N}^{(\mathcal{P})} \to \mathbb{N},\ N \mapsto (\mathrm{ord}_p(N))_{p\in\mathcal{P}} \mapsto \Lambda(N) := \textstyle\sum_{p\in\mathcal{P}}(p-1)\,\mathrm{ord}_p(N); \tag{45}$$

hence $\Lambda(1) = 0,$ and $\Lambda(M * N) = \Lambda(M) + \Lambda(N)$. The obvious inequality

$$1 + (p-1)m < (1+p-1)^m = p^m \text{ for } m \geq 2 \text{ implies } \Lambda(N) \leq N-1 \text{ and}$$
$$\Lambda(N) = N-1 \ \Leftrightarrow\ N = 1 \text{ or } N \text{ is prime.}$$

THEOREM 63. *Let G be an abelian group of exponent d and order N. Then*

$$\mu(\mathrm{Four}_G) \leq N\Lambda(N) \leq N(N-1).$$

The equality $N(N-1) = N\Lambda(N)$ holds if and only if G is simple or zero.

Proof. Choose a Jordan–Hölder series of G, the corresponding diagrams (31) as those in (32), and the FFT-algorithms derived from these diagrams. Then the numbers e_ϱ are exactly the prime factors of $N = e_1 * \cdots * e_r$ and

$$\Lambda(e_\varrho) = e_\varrho - 1,\ \Lambda(N) = \Lambda(e_1 * \cdots * e_r) = \textstyle\sum_\varrho \Lambda(e_\varrho) = \sum_\varrho (e_\varrho - 1);\ \text{hence}$$
$$\mu(\mathrm{Four}_G) \leq N(e_1 - 1 + \cdots + e_r - 1) = N\Lambda(N). \qquad \square$$

Examples 64. Let G be a group of order N.

(1) The first standard case was that of Cooley and Tukey [18]:

$$N = 2^r,\ \Lambda(N) = (2-1) * r = r,\ \mu(\mathrm{Four}_G) \leq 2^r * r = N\log_2(N).$$

(2)

$$N = 675 = 3^3 * 5^2,\ \Lambda(N) = (3-1) * 3 + (5-1) * 2 = 14 \text{ and}$$
$$N\Lambda(N) = 675 * 14 = 9450 < N(N-1) = 454950,$$

(3) $G := \mathbb{Z}/\mathbb{Z}2^{10} \times \mathbb{Z}/\mathbb{Z}2^{10},\ N = 2^{20}$. This group can be considered as a lattice with approximately one million points and may, for instance, be used for digital image processing. The direct computation of Four_G has complexity $N(N-1) \sim 2^{40}$, whereas that of the FFT is $20 * 2^{20} = 1,25 * 2^{24}$. The improvement of the complexity is dramatic.

6. The FFT in the standard cases. Assumption 29 remains in force. In this section we derive the standard special cases of the FFT and start with that of a cyclic group $G = \mathbb{Z}/\mathbb{Z}n$ of exponent $d > 0$, i.e., with $n \mid d$. As usual in the engineering literature we often identify

$$\mathbb{Z}/\mathbb{Z}n = \{0, 1, \ldots, n-1\},\ k = \overline{k},\ 0 \leq k \leq n-1, \tag{46}$$

and emphasize that the necessary care has to be taken in context with this identification. For $G = \mathbb{Z}/\mathbb{Z}n$ we choose

$$\widehat{G} := G = \mathbb{Z}/\mathbb{Z}n, \langle\overline{k}, \overline{l}\rangle := \zeta^{kld/n},\ \overline{k}, \overline{l} \in \mathbb{Z}/\mathbb{Z}n, \tag{47}$$

according to Theorem 2. A factorization $n = n_1 n_2$ of n gives rise to the exact sequence with a natural section $\sigma : \mathbb{Z}/\mathbb{Z}n_2 \to \mathbb{Z}/\mathbb{Z}n$:

(48)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/\mathbb{Z}n_1 & \xrightarrow{\text{inj}} & \mathbb{Z}/\mathbb{Z}n & \xrightarrow{\text{can}} & \mathbb{Z}/\mathbb{Z}n_2 & \longrightarrow & 0 \\ & & \| & & \| & & \|, & & \\ & & \{0,\ldots,n_1-1\} & & \{0,\ldots,n-1\} & & \{0,\ldots,n_2-1\} & & \end{array},$$

where $\mathrm{inj}(\overline{k_1}) := \overline{k_1 n_2}$, $\mathrm{can}(\overline{k}) := \overline{k}$, $\sigma(\overline{k_2}) := \overline{k_2}$ if $0 \leq k_2 \leq n_2 - 1$. For $\overline{k} \in \mathbb{Z}/\mathbb{Z}n$ and $\overline{k_2} \in \mathbb{Z}/\mathbb{Z}n_2$ the equations

$$\langle \mathrm{can}(\overline{k}), \overline{k_2} \rangle_{\mathbb{Z}/\mathbb{Z}n_2} = \zeta^{kk_2 d/n_2} = \zeta^{k(k_2 n_1)d/n} = \langle \overline{k}, \mathrm{inj}(\overline{k_2}) \rangle_{\mathbb{Z}/\mathbb{Z}n}$$

prove $\mathrm{can}^\star(\overline{k_2}) = \mathrm{inj}(\overline{k_2})$; hence

$$\begin{gathered} (\mathrm{can} : \mathbb{Z}/\mathbb{Z}n \to \mathbb{Z}/\mathbb{Z}n_2)^\star = \mathrm{inj} : \mathbb{Z}/\mathbb{Z}n_2 \to \mathbb{Z}/\mathbb{Z}n \text{ and} \\ (\mathrm{inj} : \mathbb{Z}/\mathbb{Z}n_1 \to \mathbb{Z}/\mathbb{Z}n)^\star = \mathrm{can} : \mathbb{Z}/\mathbb{Z}n \to \mathbb{Z}/\mathbb{Z}n_1, \end{gathered} \tag{49}$$

the second equality following from the first by means of $\mathrm{inj}^\star = (\mathrm{can}^\star)^\star = \mathrm{can}$. Now assume that a factorization of d is given from which we derive the following data:

$$\begin{gathered} d = e_1 * \cdots * e_r,\ d_1(i) := e_1 * \cdots * e_i,\ i = 0, \ldots, r;\ \text{hence} \\ d_1(0) = 1,\ d_1(i) = d_1(i-1) * e_i, \\ d_2(j) := d/d_1(j) = e_{j+1} * \cdots * e_r,\ j = r, \ldots, 0, \\ d_2(r) = 1,\ d_2(j-1) = d_2(j) * e_j. \end{gathered} \tag{50}$$

From (50) and by means of (48) we construct commutative exact diagrams of the type (53):

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ & & 0 & & & & \mathbb{Z}/\mathbb{Z}e_i & & \\ & & \downarrow & & & & \downarrow{\scriptstyle \gamma_i = \mathrm{inj}} & & \\ 0 & \longrightarrow & \mathbb{Z}/\mathbb{Z}d_1(i-1) & \xrightarrow{\alpha_{i-1}=\mathrm{inj}} & \mathbb{Z}/\mathbb{Z}d & \xrightarrow{\lambda_{i-1}=\mathrm{can}} & \mathbb{Z}/\mathbb{Z}d_2(i-1) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta_i = \mathrm{inj}} & & \| & & \downarrow{\scriptstyle \nu_i = \mathrm{can}} & & \\ 0 & \longrightarrow & \mathbb{Z}/\mathbb{Z}d_1(i) & \xrightarrow{\alpha_i=\mathrm{inj}} & \mathbb{Z}/\mathbb{Z}d & \xrightarrow{\lambda_i=\mathrm{can}} & \mathbb{Z}/\mathbb{Z}d_2(i) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mu_i = \mathrm{can}} & & & & \downarrow & & \\ & & \mathbb{Z}/\mathbb{Z}e_i & & & & 0 & & \\ & & \downarrow & & & & & & \\ & & 0 & & & & & & \end{array} \tag{51}$$

with the natural sections σ from (48) in $\mathbb{Z}/\mathbb{Z}d_1(i) \underset{\sigma_i=\sigma}{\overset{\mu_i=\mathrm{can}}{\rightleftarrows}} \mathbb{Z}/\mathbb{Z}e_i$. Application of the exact duality functor $H \mapsto \widehat{H} = H$ to the cyclic groups of the preceding diagram and

the identities (49) yield the dual commutative exact diagrams of the type (34):

$$
\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & & & \mathbb{Z}/\mathbb{Z}e_j & & \\
 & & \downarrow & & & & \downarrow{\scriptstyle \mu_j^\star=\mathrm{inj}} & & \\
0 & \longrightarrow & \mathbb{Z}/\mathbb{Z}d_2(j) & \xrightarrow{\lambda_j^\star=\mathrm{inj}} & \mathbb{Z}/\mathbb{Z}d & \xrightarrow{\alpha_j^\star=\mathrm{can}} & \mathbb{Z}/\mathbb{Z}d_1(j) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \nu_j^\star=\mathrm{inj}} & & \| & & \downarrow{\scriptstyle \beta_j^\star=\mathrm{can}} & & \\
0 & \longrightarrow & \mathbb{Z}/\mathbb{Z}d_2(j-1) & \xrightarrow{\lambda_{j-1}^\star=\mathrm{inj}} & \mathbb{Z}/\mathbb{Z}d & \xrightarrow{\alpha_{j-1}^\star=\mathrm{can}} & \mathbb{Z}/\mathbb{Z}d_1(j-1) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \gamma_j^\star=\mathrm{can}} & & & & \downarrow & & \\
 & & \mathbb{Z}/\mathbb{Z}e_j & & & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}
\tag{52}
$$

with the natural sections $\widehat{\sigma}$ from (48) in $\mathbb{Z}/\mathbb{Z}d_2(j-1) \underset{\widehat{\sigma}_j=\sigma}{\overset{\gamma_j^\star=\mathrm{can}}{\rightleftarrows}} \mathbb{Z}/\mathbb{Z}e_j$. According to Lemma 55 the diagram (51) gives rise to the index bijection

$$
\begin{array}{c}
\mathrm{ind} : \prod_{i=1}^r \mathbb{Z}/\mathbb{Z}e_i = \prod_{i=1}^r \{0, \cdots, e_i - 1\} \cong \mathbb{Z}/\mathbb{Z}d = \{0, \cdots, d-1\}, \\
\mathrm{ind}(k_1, \cdots, k_r) = \sum_{i=1}^r \alpha_i \sigma_i(k_i) = \sum_{i=1}^r k_i d/d_1(i) \\
= \sum_{i=1}^r k_i d_2(i) = \sum_{i=1}^r k_i * e_{i+1} * \cdots * e_r.
\end{array}
\tag{53}
$$

Likewise, the diagram (52) induces the bijection

$$
\begin{array}{c}
\widehat{\mathrm{ind}} : \prod_{j=1}^r \mathbb{Z}/\mathbb{Z}e_j = \prod_{j=1}^r \{0, \cdots, e_j - 1\} \cong \mathbb{Z}/\mathbb{Z}d = \{0, \cdots, d-1\}, \\
\widehat{\mathrm{ind}}(\widehat{k}_1, \cdots, \widehat{k}_r) = \sum_{j=1}^r \lambda_{j-1}^\star \widehat{\sigma}_j(\widehat{k}_j) = \sum_{j=1}^r \widehat{k}_j d/d_2(j-1) \\
= \sum_{j=1}^r \widehat{k}_j * e_1 * \cdots * e_{j-1}.
\end{array}
\tag{54}
$$

Corollary 65. *The unique representation*

$$n = \sum_{i=1}^r k_i * e_{i+1} * \cdots * e_r,\ 0 \le n < d,\ 0 \le k_i < e_i,\ i = 1, \ldots, r,$$

according to (53) *is obtained by recursion with respect to* i *as*

$$n_r := n,\ n_i := n_{i-1} * e_i + k_i,\ 0 \le k_i < e_i,\ i = r, \ldots, 1.$$

Likewise, the unique representation

$$n = \sum_{j=1}^r \widehat{k}_j * e_1 * \cdots * e_{j-1},\ 0 \le n < d,\ 0 \le \widehat{k}_j < e_j,\ j = 1, \ldots, r,$$

according to (54) *is obtained by induction with respect to* j *as*

$$\widehat{n}_0 := n,\ \widehat{n}_{j-1} = \widehat{n}_j * e_j + \widehat{k}_j,\ 0 \le \widehat{k}_j < e_j,\ j = 1, \ldots, r.$$

Proof. The proof is the same as that of the q-adic representation of a natural number for $q > 1$. For instance,

$$d > n =: n_r := n_{r-1} * e_r + k_r,\ 0 \le k_r < e_r,\ n_{r-1} \le \tfrac{n}{e_r} < \tfrac{d}{e_r} = e_1 * \cdots * e_{r-1},$$
$$d > n =: \widehat{n}_0 = \widehat{n}_1 * e_1 + \widehat{k}_1,\ 0 \le \widehat{k}_1 < e_1,\ \widehat{n}_1 < e_2 * \cdots * e_r. \qquad \square$$

For vectors $(k_i; \widehat{k}_1, \cdots, \widehat{k}_i)$ with components $k_i,\ \widehat{k}_i \in \mathbb{Z}/\mathbb{Z}e_i = \{0, \cdots, e_i - 1\}$ the function φ_i according to (37) is defined by

(55)
$$\varphi_i(k_i; \widehat{k}_1, \cdots, \widehat{k}_i) = \left\langle \alpha_i \sigma_i(k_i), \textstyle\sum_{j=1}^{i} \lambda_{j-1}^{\star} \widehat{\sigma}_j(\widehat{k}_j) \right\rangle$$
$$= \left\langle k_i d/d_1(i), \textstyle\sum_{j=1}^{i} \widehat{k}_j d/d_2(j-1) \right\rangle = \zeta^{\varepsilon_i(k_i; \widehat{k}_1, \cdots, \widehat{k}_i)}, \text{ where}$$
$$\varepsilon_i(k_i; \widehat{k}_1, \cdots, \widehat{k}_i) := k_i * e_{i+1} * \cdots * e_r * \textstyle\sum_{j=1}^{i} \widehat{k}_j * e_1 * \cdots * e_{j-1},\ 0 \le k_i,\ \widehat{k}_i < e_i.$$

Similarly the function $\widehat{\varphi}_j$ from (38) has the form

(56)
$$\widehat{\varphi}_j(k_j, \cdots, k_r; \widehat{k}_j) = \zeta^{\widehat{\varepsilon}_j(k_j, \cdots, k_r; \widehat{k}_j)},\ j = 1, \cdots, r, \text{ where}$$
$$\widehat{\varepsilon}_j(k_j, \cdots, k_r; \widehat{k}_j) := \widehat{k}_j * e_1 * \cdots * e_{j-1} * \textstyle\sum_{i=j}^{r} k_i * e_{i+1} * \cdots * e_r,\ 0 \le k_i,\ \widehat{k}_i < e_i.$$

Theorem 58 applied to the preceding situation now implies the following theorem.

THEOREM 66 (FFT for cyclic groups [8, pp. 188–191]). *Consider a number $d > 0$ with a factorization $d = e_1 * \cdots * e_r$, the cyclic group $G := \mathbb{Z}/\mathbb{Z}d$, and the associated DFT*

$$\mathrm{Four}_{\mathbb{Z}/\mathbb{Z}d} : K^{\mathbb{Z}/\mathbb{Z}d} = K^{\{0, \cdots, d-1\}} = K^d \to K^d,\ a \mapsto \widehat{a},$$
$$\widehat{a}(l) := \textstyle\sum_{k=0}^{d-1} a(k) \zeta^{kl},\ 0 \le l < d.$$

1. *The following "decimation in time" algorithm computes $\widehat{a}$ from a with complexity $d(e_1 + \cdots + e_r - r)$. Inductively define functions*

$$a_\varrho : \textstyle\prod_{i=1}^{r} \{0, \cdots, e_i - 1\} \to K \text{ for } \varrho = 0, \ldots, r \text{ by}$$
$$a_0(k_1, \cdots, k_r) := a\left(\textstyle\sum_{i=1}^{r} k_i * e_{i+1} * \cdots * e_r\right),$$
$$a_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r) := \textstyle\sum_{k_\varrho=0}^{e_\varrho - 1} a_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r) \zeta^{\varepsilon_\varrho(k_\varrho; \widehat{k}_1, \cdots, \widehat{k}_\varrho)}$$

with ε_ϱ from (55). *Then*

$$\widehat{a}(l) = a_r(\widehat{k}_1, \cdots, \widehat{k}_r) \text{ for } l = \textstyle\sum_{j=1}^{r} \widehat{k}_j * e_1 * \cdots * e_{j-1},\ 0 \le l < d, 0 \le \widehat{k}_j < e_j.$$

2. *The following "decimation in frequency" algorithm also computes $\widehat{a}$ with complexity $d(e_1 + \cdots + e_r - r)$. Recursively define functions*

$$b_\varrho : \textstyle\prod_{\varrho=1}^{r} \{0, \cdots, e_\varrho - 1\} \to K \text{ for } \varrho = r, \ldots, 0 \text{ by}$$
$$b_r(\widehat{k}_1, \cdots, \widehat{k}_r) := a\left(\textstyle\sum_{j=1}^{r} \widehat{k}_j * e_1 * \cdots * e_{j-1}\right),$$
$$b_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r) = \textstyle\sum_{\widehat{k}_\varrho=0}^{e_\varrho - 1} b_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r) \zeta^{\widehat{\varepsilon}_\varrho(k_\varrho, \cdots, k_r; \widehat{k}_\varrho)}$$

with $\widehat{\varepsilon}_\varrho$ from (56). *Then*

$$\widehat{a}(k) = b_0(k_1, \cdots, k_r) \text{ for } k = \textstyle\sum_{i=1}^{r} k_i * e_{i+1} * \cdots * e_r, 0 \le k < d, 0 \le k_i < e_i.$$

Example 67. In the situation of the preceding theorem we choose

$$K := \mathbb{C},\ d = 6 = 2 * 3,\ G := \mathbb{Z}/\mathbb{Z}6 = \{0, \cdots, 5\},$$
$$\zeta := \exp(2\pi i/6) = 1/2 + i\sqrt{3}/2,\ \zeta^6 = 1,$$
$$\widehat{a}(l) = \textstyle\sum_{k=0}^{5} a(k)\zeta^{kl},\ 0 \le k, l \le 5.$$

The FFT-algorithm of the preceding theorem computes $\widehat{a}$ from $a = (a(0), \cdots, a(5))$ with $6 * (2 + 3 - 2) = 18$ elementary computation steps. The root ζ satisfies the cyclotomic equation $\phi_6(\zeta) = \zeta^2 - \zeta + 1 = 0$ or $\zeta^2 = \zeta - 1$, hence the group table

k	0	1	2	3	4	5
ζ^k	1	ζ	$\zeta - 1$	-1	$-\zeta$	$-\zeta + 1$

The index functions are

$$\mathrm{ind}(k_1, k_2) = k_1 * e_2 + k_2 = 3k_1 + k_2 \text{ and}$$
$$\widehat{\mathrm{ind}}(\widehat{k}_1, \widehat{k}_2) = \widehat{k}_1 + \widehat{k}_2 * e_1 = \widehat{k}_1 + 2\widehat{k}_2, \quad 0 \le k_1, \widehat{k}_1 \le 1,\ 0 \le k_2, \widehat{k}_2 \le 2.$$

The values of ind and $\widehat{\mathrm{ind}}$ are given in the following table:

(k_1, k_2)	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$\mathrm{ind}(k_1, k_2)$	0	1	2	3	4	5
$\widehat{\mathrm{ind}}(k_1, k_2)$	0	2	4	1	3	5

The value table of $a_0 := a \circ \mathrm{ind}$ is

(k_1, k_2)	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$a_0(k_1, k_2)$	$a(0)$	$a(1)$	$a(2)$	$a(3)$	$a(4)$	$a(5)$

For the computation of a_1 we need the exponent ε_1, where

$$\varepsilon_1(k_1; \widehat{k}_1) = k_1 * \widehat{k}_1 * e_2 = 3k_1\widehat{k}_1,\ \varepsilon_1(0; \widehat{k}_1) = 0,\ \varepsilon_1(1; \widehat{k}_1) = 3\widehat{k}_1,$$
$$a_1(\widehat{k}_1, k_2) = a_0(0, k_2) + a_0(1, k_2)\zeta^{3\widehat{k}_1}.$$

In detail we get

$$\begin{array}{lllllllll}
a_1(0,0) & = & a_0(0,0) & + & a_0(1,0) & = & a(0) & + & a(3), \\
a_1(0,1) & = & a_0(0,1) & + & a_0(1,1) & = & a(1) & + & a(4), \\
a_1(0,2) & = & a_0(0,2) & + & a_0(1,2) & = & a(2) & + & a(5), \\
a_1(1,0) & = & a_0(0,0) & + & a_0(1,0)\zeta^3 & = & a(0) & - & a(3), \\
a_1(1,1) & = & a_0(0,1) & - & a_0(1,1)\zeta^3 & = & a(1) & - & a(4), \\
a_1(1,2) & = & a(0,2) & - & a_0(1,2)\zeta^3 & = & a(2) & - & a(5).
\end{array}$$

For the computation of a_2 we need ε_2, where

$$\varepsilon_2(k_2; \widehat{k}_1; \widehat{k}_2) = k_2(\widehat{k}_1 + 2\widehat{k}_2),$$
$$a_2(\widehat{k}_1, \widehat{k}_2) = a_1(\widehat{k}_1, 0) + a_1(\widehat{k}_1, 1)\zeta^{\widehat{k}_1 + 2\widehat{k}_2} + a_1(\widehat{k}_1, 2)\zeta^{2(\widehat{k}_1 + 2\widehat{k}_2)}.$$

In detail, we obtain

$$\begin{aligned}
\widehat{a}(0) = a_2(0,0) &= a_1(0,0) + a_1(0,1) + a_1(0,2)\\
&= a(0) + a(3) + a(1) + a(4) + a(2) + a(5) = \textstyle\sum_{i=0}^{5} a(i)\zeta^{i*0},\\
\widehat{a}(2) = a_2(0,1) &= a_1(0,0) + a_1(0,1)\zeta^2 + a_1(0,2)\zeta^4\\
&= a(0) + a(3) + (a(1) + a(4))\zeta^2 + (a(2) + a(5))(-\zeta)\\
&= a(0) + a(1)\zeta^2 + a(2)(-\zeta) + a(3) + a(4)\zeta^2 + a(5)(-\zeta)\\
&= \textstyle\sum_{i=0}^{5} a(i)\zeta^{i*2},\\
\widehat{a}(4) = a_2(0,2) &= a_1(0,0) + a_1(0,1)\zeta^4 + a_1(0,2)\zeta^8\\
&= (a(0) + a(3)) + (a(1) + a(4))(-\zeta) + (a(2) + a(5))\zeta^2\\
&= a(0) + a(1)(-\zeta) + a(2)\zeta^2 + a(3) + a(4)(-\zeta) + a(5)\zeta^2\\
&= \textstyle\sum_{i=0}^{5} a(i)\zeta^{i*4},\\
\widehat{a}(1) = a_2(1,0) &= a_1(1,0) + a_1(1,1)\zeta^1 + a_1(1,2)\zeta^2\\
&= (a(0) - a(3)) + (a(1) - a(4))\zeta + (a(2) - a(5))\zeta^2\\
&= a(0) + a(1)\zeta + a(2)\zeta^2 + a(3)(-1) + a(4)(-\zeta) + a(5)(-\zeta^2)\\
&= \textstyle\sum_{i=0}^{5} a(i)\zeta^{i*1},\\
\widehat{a}(3) = a_2(1,1) &= a_1(1,0) + a_1(1,1)\zeta^3 + a_1(1,2)\zeta^6\\
&= (a(0) - a(3)) + (a(1) - a(4))(-1) + (a(2) - a(5))\\
&= a(0) + a(1)(-1) + a(2) + a(3)(-1) + a(4) + a(5)(-1)\\
&= \textstyle\sum_{i=0}^{5} a(i)\zeta^{i*3},\\
\widehat{a}(5) = a_2(1,2) &= a_1(1,0) + a_1(1,1)\zeta^5 + a_1(1,2)\zeta^{10}\\
&= (a(0) - a(3)) + (a(1) - a(4))(-\zeta^2) + (a(2) - a(5))(-\zeta)\\
&= a(0) + a(1)(-\zeta^2) + a(2)(-\zeta) + a(3)(-1) + a(4)\zeta^2 + a(5)\zeta\\
&= \textstyle\sum_{i=0}^{5} a(i)\zeta^{i*5}.
\end{aligned}$$

In the following corollary we assume that d in Theorem 66 is a power of a number q; i.e.,

$$d = q^r,\ q > 1,\ r > 1,\ e_1 = \cdots = e_r = q,\ d_1(i) = q^i,\ d_2(i) = q^{r-i}. \tag{57}$$

The associated index functions according to (53) and (54) are

$$\begin{aligned}
\mathrm{ind}(k_1, \cdots, k_r) &= \textstyle\sum_{i=1}^{r} k_i q^{r-i} = \sum_{j=1}^{r} k_{r+1-j} q^{j-1}, 0 \le k_i < q,\\
\widehat{\mathrm{ind}}(\widehat{k}_1, \cdots, \widehat{k}_r) &= \textstyle\sum_{j=1}^{r} \widehat{k}_j q^{j-1},\ 0 \le \widehat{k}_j < q,
\end{aligned} \tag{58}$$

and they give the q-adic representation of a natural number. The map

$$\begin{aligned}
\widehat{\mathrm{ind}}^{-1} \circ \mathrm{ind} = \mathrm{ind}^{-1} \circ \widehat{\mathrm{ind}} : \{0, \cdots, q-1\}^r &\to \{0, \cdots, q-1\}^r,\\
(k_1, \cdots, k_r) &\mapsto (k_r, \cdots, k_1),
\end{aligned} \tag{59}$$

is usually called the *bit reversal map* for an obvious reason. The functions ε_i and $\widehat{\varepsilon}_j$ from (55) and (56) are

(60)

$$\varepsilon_i(k_i; \widehat{k}_1, \cdots, \widehat{k}_i) = \textstyle\sum_{j=1}^{i} k_i \widehat{k}_j q^{j-1+r-i}, \quad \widehat{\varepsilon}_j(k_j, \cdots, k_r; \widehat{k}_j) = \sum_{i=j}^{r} k_i \widehat{k}_j q^{j-1+r-i}.$$

COROLLARY 68. *Consider natural numbers $q > 1,\ r > 1,$ and $d := q^r$, the cyclic group $G := \mathbb{Z}/\mathbb{Z}q^r$, and the DFT*

$$\mathrm{Four}_{\mathbb{Z}/\mathbb{Z}q^r} K^G = K^{q^r} \to K^{q^r},\ a \mapsto \widehat{a},\ \widehat{a}(l) := \sum_{k=0}^{q^r-1} a(k)\zeta^{kl},\ 0 \le l < q^r.$$

1. *The following "decimation in time" algorithm computes $\widehat{a}$ from a with complexity $q^r(q-1)r$. Inductively define functions*

$$a_\varrho : \{0, \cdots, q-1\}^r \to K \text{ for } \varrho = 0, \ldots, r \text{ by}$$
$$a_0(k_1, \cdots, k_r) := a\left(\sum_{i=1}^r k_i q^{r-i}\right),$$
$$a_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r) := \sum_{k_\varrho=0}^{q-1} a_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r)\zeta^{\varepsilon_\varrho(k_\varrho;\widehat{k}_1, \cdots, \widehat{k}_\varrho)}$$

with ε_ϱ from (60). *Then*

$$\widehat{a}(l) = a_r(\widehat{k}_1, \cdots, \widehat{k}_r) \text{ for } l = \sum_{j=1}^r \widehat{k}_j q^{j-1},\ 0 \le l < q^r,\ 0 \le \widehat{k}_j < q.$$

2. *The following "decimation in frequency" algorithm also computes $\widehat{a}$ with complexity $q^r(q-1)r$. Recursively define functions*

$$b_\varrho : \{0, \cdots, q-1\}^r \to K \text{ for } \varrho = r, \ldots, 0 \text{ by}$$
$$b_r(\widehat{k}_1, \cdots, \widehat{k}_r) := a\left(\sum_{j=1}^r \widehat{k}_j q^{j-1}\right),$$
$$b_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r) = \sum_{\widehat{k}_\varrho=0}^{q-1} b_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r)\zeta^{\widehat{\varepsilon}_\varrho(k_\varrho, \cdots, k_r;\widehat{k}_\varrho)}$$

with $\widehat{\varepsilon}_\varrho$ from (60). *Then*

$$\widehat{a}(k) = b_0(k_1, \cdots, k_r) \text{ for } k = \sum_{i=1}^r k_i q^{r-i}, 0 \le k < q^r, 0 \le k_i < q.$$

COROLLARY 69. (see [18]) *In the situation of Corollary* 68 *assume that $q = 2$ and $G = \mathbb{Z}/\mathbb{Z}2^r$. The FFT-algorithms reduce to the following algorithms. The functions $a, \widehat{a}$ and a_ϱ, b_ϱ belong to K^{2^r} (resp., $K^{\{0,1\}^r}$).*

1. *The following "decimation in time" algorithm computes $\widehat{a}$ from a with complexity $r * 2^r$. Inductively define functions*

$$a_\varrho : \{0,1\}^r \to K \text{ for } \varrho = 0, \ldots, r \text{ by}$$
$$a_0(k_1, \cdots, k_r) := a\left(\sum_{i=1}^r k_i 2^{r-i}\right),$$
$$a_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r)$$
$$:= a_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, 0, k_{\varrho+1}, \cdots, k_r) + a_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, 1, k_{\varrho+1}, \cdots, k_r)\zeta^{\varepsilon_\varrho(1;\widehat{k}_1, \cdots, \widehat{k}_\varrho)}$$

with $\varepsilon_\varrho(1; \widehat{k}_1, \cdots, \widehat{k}_\varrho) := \sum_{j=1}^\varrho \widehat{k}_j 2^{j-1+r-\varrho}$. Then

$$\widehat{a}(l) = a_r(\widehat{k}_1, \cdots, \widehat{k}_r) \text{ for } l = \sum_{j=1}^r \widehat{k}_j 2^{j-1},\ 0 \le l < 2^r, 0 \le \widehat{k}_j \le 1.$$

2. *The following "decimation in frequency" algorithm also computes $\widehat{a}$ with complexity $r * 2^r$. Recursively define functions*

$$b_\varrho : \{0,1\}^r \to K \text{ for } \varrho = r, \ldots, 0 \text{ by}$$
$$b_r(\widehat{k}_1, \cdots, \widehat{k}_r) := a\left(\sum_{j=1}^r \widehat{k}_j 2^{j-1}\right),$$
$$b_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r)$$
$$= b_\varrho(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, 0, k_{\varrho+1}, \cdots, k_r) + b_\varrho(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, 1, k_{\varrho+1}, \cdots, k_r)\zeta^{\widehat{\varepsilon}_\varrho(k_\varrho, \cdots, k_r;1)}$$

with $\widehat{\varepsilon}_\varrho(k_\varrho, \cdots, k_r; 1) := \sum_{i=\varrho}^r k_i 2^{\varrho-1+r-i}$. *Then*

$$\widehat{a}(k) = b_0(k_1, \cdots, k_r) \text{ for } k = \textstyle\sum_{i=1}^r k_i 2^{r-i},\ 0 \le k < 2^r,\ 0 \le k_i \le 1.$$

Observe that the computation of $a_\varrho(\widehat{k}_1, \cdots, \widehat{k}_\varrho, k_{\varrho+1}, \cdots, k_r)$ (*resp., of* $b_{\varrho-1}(\widehat{k}_1, \cdots, \widehat{k}_{\varrho-1}, k_\varrho, \cdots, k_r)$) *from* $a_{\varrho-1}$ (*resp.,* b_ϱ) *requires just one elementary computation step* $\alpha + \lambda\beta$.

For the next application of Theorem 58 we assume that a direct decomposition of the group G, i.e., an isomorphism

$$\varphi : \textstyle\prod_{i=1}^r K_i \cong G, \tag{61}$$

is given. For every subset I of $\{1, \cdots, r\}$ we define

$$G(I) := \textstyle\prod_{i\in I} K_i, \text{ especially } G_i := G(\{1, \cdots, i\}), H_i := G(\{i+1, \cdots, r\}). \tag{62}$$

For $J \subseteq I$ there results the exact sequence

$$\begin{gathered} 0 \to G(J) \xrightarrow{\text{inj}} G(I) \xrightarrow{\text{proj}} G(I \setminus J) \to 0, \\ \text{inj}((l_j)_{j\in J}) := (k_i)_{i\in I}, \text{ where } k_i := \begin{cases} l_i & \text{if } i \in J \\ 0 & \text{if } i \in I \setminus J, \end{cases} \\ \text{proj}((k_i)_{i\in I}) := (k_i)_{i\in I\setminus J}, \end{gathered} \tag{63}$$

where, moreover, $\text{inj} : G(I \setminus J) \to G(I)$ is a *homomorphic* section of the canonical projection proj. The groups $\widehat{K_i}$ and the forms $\langle -, - \rangle_{K_i}$ being given arbitrarily, we now choose

$$\widehat{G(I)} := \textstyle\prod_{i\in I} \widehat{K_i}, \quad \langle (k_i)_{i\in I}, (\widehat{k}_i)_{i\in I} \rangle := \textstyle\prod_{i\in I} \langle k_i, \widehat{k}_i \rangle_{K_i}. \tag{64}$$

It is then easily seen that

$$\begin{aligned} (\text{inj} : G(J) \to G(I))^\star &= \text{proj} : \widehat{G(I)} \to \widehat{G(J)}, \\ (\text{proj} : G(I) \to G(J))^\star &= \text{inj} : \widehat{G(J)} \to \widehat{G(I)}. \end{aligned} \tag{65}$$

The isomorphism φ from (61) and the exact sequences (63) and (65) now imply the exact sequences

$$\begin{aligned} 0 \to G_i &\xrightarrow{\varphi \circ \text{inj}} G \xrightarrow{\text{proj} \circ \varphi^{-1}} H_i \to 0, \\ 0 \to \widehat{H_i} &\xrightarrow{(\varphi^\star)^{-1} \circ \text{inj}} \widehat{G} \xrightarrow{\text{proj} \circ \varphi^\star} \widehat{G_i} \to 0. \end{aligned} \tag{66}$$

Finally we use these data to construct the diagrams (32) and (34) in the form

(67)
$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & & & K_i & & \\
 & & \downarrow & & & & \downarrow{\scriptstyle \gamma_i:=\mathrm{inj}} & & \\
0 & \longrightarrow & G_{i-1} & \xrightarrow{\alpha_{i-1}:=\varphi\circ\mathrm{inj}} & G & \xrightarrow{\lambda_{i-1}:=\mathrm{proj}\circ\varphi^{-1}} & H_{i-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta_i:=\mathrm{inj}} & & \| & & \downarrow{\scriptstyle \nu_i:=\mathrm{proj}} & & \\
0 & \longrightarrow & G_i & \xrightarrow{\alpha_i:=\varphi\circ\mathrm{inj}} & G & \xrightarrow{\lambda_i:=\mathrm{proj}\circ\varphi^{-1}} & H_i & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mu_i:=\mathrm{proj}} & & & & \downarrow & & \\
 & & K_i & & & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

(68)
$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & & & \widehat{K_j} & & \\
 & & \downarrow & & & & \downarrow{\scriptstyle \mu_j^\star:=\mathrm{inj}} & & \\
0 & \longrightarrow & \widehat{H_j} & \xrightarrow{\lambda_j^\star:=(\varphi^\star)^{-1}\circ\mathrm{inj}} & \widehat{G} & \xrightarrow{\alpha_j^\star:=\mathrm{proj}\circ\varphi^\star} & \widehat{G_j} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \nu_j^\star:=\mathrm{inj}} & & \| & & \downarrow{\scriptstyle \beta_j^\star:=\mathrm{proj}} & & \\
0 & \longrightarrow & \widehat{H_{j-1}} & \xrightarrow{\lambda_{j-1}^\star:=(\varphi^\star)^{-1}\circ\mathrm{inj}} & \widehat{G} & \xrightarrow{\alpha_{j-1}^\star:=\mathrm{proj}\circ\varphi^\star} & \widehat{G_{j-1}} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \gamma_j^\star:=\mathrm{proj}} & & & & \downarrow & & \\
 & & \widehat{K_j} & & & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

with the canonical homomorphic sections

$$\sigma_i := \mathrm{inj} : K_i \to G_i = \textstyle\prod_{k=1}^{i} K_k \text{ and } \widehat{\sigma}_j := \mathrm{inj} : \widehat{K_j} \to \widehat{H_{j-1}} = \textstyle\prod_{k=j}^{r} \widehat{K_k}. \tag{69}$$

These diagrams induce the index transformations ind and $\widehat{\mathrm{ind}}$ from Corollaries 55 and 56; indeed

$$\begin{array}{c}
\mathrm{ind}((k_i)_{i=1,\cdots,r}) = \sum_{i=1}^{r} \alpha_i\sigma_i(k_i) = \varphi\left(\sum_{i=1}^{r} \mathrm{inj}\circ\mathrm{inj}(k_i)\right) \\
= \varphi\left(\sum_{i=1}^{r}(0,\cdots,0,k_i,0,\cdots,0)\right) = \varphi((k_i)_{i=1,\cdots,r}),
\end{array}$$

and hence

$$\mathrm{ind} = \varphi : \textstyle\prod_{i=1}^{r} K_i \cong G \text{ and likewise } \widehat{\mathrm{ind}} = (\varphi^\star)^{-1} : \prod_{j=1}^{r} \widehat{K_j} \cong \widehat{G}. \tag{70}$$

Also, with the notation from (35), we have

$$\begin{gathered}\operatorname{fact}_{ij}(k,\widehat{k}) = \langle \alpha_i\sigma_i(k_i), \lambda^\star_{j-1}\widehat{\sigma}_j(\widehat{k}_j)\rangle \\ = \langle \varphi\operatorname{inj}(k_i), (\varphi^\star)^{-1}\operatorname{inj}(\widehat{k}_j)\rangle = \langle \varphi^{-1}\varphi\operatorname{inj}(k_i), \operatorname{inj}(\widehat{k}_j)\rangle \\ = \langle (0,\cdots,0,k_i,0,\cdots,0),(0,\cdots,0,\widehat{k}_j,0,\cdots,0)\rangle = \begin{cases}\langle k_i,\widehat{k}_i\rangle & \text{if } i=j,\\ 1 & \text{if } i\neq j,\end{cases} \text{ and hence} \\ \varphi_\varrho(k_\varrho;\widehat{k}_1,\cdots,\widehat{k}_\varrho) = \langle k_\varrho,\widehat{k}_\varrho\rangle,\ \varrho=1,\cdots,r.\end{gathered}$$

Theorem 58 now implies the following theorem.

THEOREM 70. *Assume that a group isomorphism $\varphi : \prod_{i=1}^r K_i \cong G$ is given. Then the following recursive algorithm computes the Fourier transform $\widehat{a} \in K^{\widehat{G}}$ of a function $a \in K^G$ with complexity $N(e_1+\cdots+e_r-r)$ where $N := \operatorname{ord}(G)$ and $e_i := \operatorname{ord}(K_i)$. Inductively define functions*

$$\begin{gathered}a_\varrho : \widehat{K_1}\times\cdots\times\widehat{K_\varrho}\times K_{\varrho+1}\times\cdots\times K_r \to K \ \text{ for } \varrho=0,\dots,r \text{ by } a_0 := a\circ\varphi \text{ and} \\ a_\varrho(\widehat{k}_1,\cdots,\widehat{k}_\varrho,k_{\varrho+1},\cdots,k_r) := \textstyle\sum_{k_\varrho\in K_\varrho} a_{\varrho-1}(\widehat{k}_1,\cdots,\widehat{k}_{\varrho-1},k_\varrho,\cdots,k_r)\langle k_\varrho,\widehat{k}_\varrho\rangle \text{ or} \\ a_\varrho(\widehat{k}_1,\cdots,\widehat{k}_{\varrho-1},-,k_{\varrho+1},\cdots,k_r) := \operatorname{Four}_{K_\varrho}\left(a_{\varrho-1}(\widehat{k}_1,\cdots,\widehat{k}_{\varrho-1},-,k_{\varrho+1},\cdots,k_r)\right). \\ \text{Then } \widehat{a} = a_r\circ\varphi^\star.\end{gathered}$$

If, in particular, $G := \prod_{i=1}^r K_i$ and $\varphi = \mathrm{id}$, then $a_0 = a$ and $\widehat{a} = a_r$.

Example 71 (Walsh–Fourier FFT). We apply the preceding theorem to $d := 2$, the group

$$G := \widehat{G} := (\mathbb{Z}/\mathbb{Z}2)^r = \{0,1\}^r \ni k = (k_1,\cdots,k_r),\ 0\le k_i\le 1,$$

of exponent 2 with the form $k\bullet l := \sum_{i=1}^r k_i l_i \in \mathbb{Z}/\mathbb{Z}2$, and a ring K in which 2 is invertible so that Assumption 29 is satisfied for $\zeta := -1$. The Walsh–Fourier DFT is given by

$$\operatorname{Four}_G : K^G \cong K^G,\ \operatorname{Four}_G(a)(\widehat{k}) := \widehat{a}(\widehat{k}_1,\cdots,\widehat{k}_r) = \textstyle\sum_{k\in G} a(k)(-1)^{k\bullet\widehat{k}}$$

and inductively computed with complexity $r*2^r$ by means of the algorithm

$$\begin{gathered}a_0 := a \text{ and for } 1\le\varrho\le r \\ a_\varrho(\widehat{k}_1,\cdots,\widehat{k}_\varrho,k_{\varrho+1},\cdots,k_r) \\ := a_{\varrho-1}(\widehat{k}_1,\cdots,\widehat{k}_{\varrho-1},0,k_{\varrho+1},\cdots,k_r) + a_{\varrho-1}(\widehat{k}_1,\cdots,\widehat{k}_{\varrho-1},1,k_{\varrho+1},\cdots,k_r)(-1)^{\widehat{k}_\varrho}, \\ \widehat{a} = a_r.\end{gathered}$$

The next example contains the prime factor algorithm according to Good.

Example 72 (the Good FFT or the prime factor algorithm [21]). In the situation of Theorem 66 assume that the numbers e_i are relatively prime. The euclidean algorithm and the Chinese remainder theorem yield representations

$$1 = r_i * e_i + s_i * d/e_i = a_i + b_i, \quad b_i := s_i * d/e_i,$$

and the group isomorphism

$$\Delta : G := \mathbb{Z}/\mathbb{Z}d \cong \textstyle\prod_{i=1}^r K_i := \prod_{i=1}^r \mathbb{Z}/\mathbb{Z}e_i,\ \bar{l}\mapsto(\bar{l},\cdots,\bar{l}).$$

The inverse map of Δ is

$$\varphi := \Delta^{-1} : \textstyle\prod_{i=1}^r \mathbb{Z}/\mathbb{Z}e_i \cong \mathbb{Z}/\mathbb{Z}d,\ \varphi(\overline{k_1},\cdots,\overline{k_r}) = \overline{\sum_{i=1}^r k_i b_i}.$$

For the application of Theorem 70 we compute $\varphi^\star$. The equations

$$\begin{gathered}\langle\varphi(\overline{k_1},\cdots,\overline{k_r}),\bar{l}\rangle=\zeta^{\sum_{i=1}^r k_i b_i l}\\ =\zeta^{\sum_{i=1}^r k_i(s_i l)d/e_i}=\prod_{i=1}^r\langle\overline{k_i},\overline{s_i l}\rangle_{K_i}=\langle\overline{k},(\overline{s_1 l},\cdots,\overline{s_r l})\rangle\end{gathered}$$

imply

$$\varphi^\star(\bar{l})=(\overline{s_1 l},\cdots,\overline{s_r l})=(\overline{s_1},\cdots,\overline{s_r})\Delta(\bar{l})\in\textstyle\prod_{i=1}^r\mathbb{Z}/\mathbb{Z}e_i.$$

Application of Theorem 70 to the preceding data now shows that the following algorithm computes $\widehat{a}\in K^G$ from $a\in K^G$ with complexity $d(e_1+\cdots+e_r-r)$. Inductively define functions

$$\begin{gathered}a_\varrho:\textstyle\prod_{i=1}^r\{0,\cdots,e_i-1\}\to K\text{ for }\varrho=0,\dots,r\text{ by}\\ a_0(k_1,\cdots,k_r):=a\left(\overline{\textstyle\sum_{i=1}^r k_i b_i}\right),\\ a_\varrho(\widehat{k}_1,\cdots,\widehat{k}_\varrho,k_{\varrho+1},\cdots,k_r):=\textstyle\sum_{k_\varrho=0}^{e_\varrho-1}a_{\varrho-1}(\widehat{k}_1,\cdots,\widehat{k}_{\varrho-1},k_\varrho,\cdots,k_r)\zeta^{k_\varrho\widehat{k}_\varrho d/e_\varrho}.\text{ Then}\\ \overline{a}(\bar{l})=a_r(\overline{s_1 l},\cdots,\overline{s_r l}),\quad \bar{l}\in\mathbb{Z}/\mathbb{Z}d.\end{gathered}$$

Consider, in particular, the case of Example 67, i.e., $d=6=e_1e_2=2*3$. Then

$$1=(-1)*2+1*6/2=2*6/3+(-1)*3;\text{ hence }s_1=1,\ b_1=3,\ s_2=2,\ b_2=4.$$

The maps

$$\varphi,\ (\varphi^\star)^{-1}:\mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}3=\{0,1\}\times\{0,1,2\}\to\mathbb{Z}/\mathbb{Z}6=\{0,1,2,3,4,5\}$$

have the value table

(k_1,k_2)	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$\varphi(k_1,k_2)$	0	4	2	3	1	5
$(\varphi^\star)^{-1}(k_1,k_2)$	0	2	4	3	5	1

Since the maps φ and $(\varphi^\star)^{-1}$ differ from the index maps ind and $\widehat{\text{ind}}$ from Example 67, the FFT-algorithms from Theorem 66 and Example 72 applied to the same case $d=e_1*\cdots*e_r$ with relatively prime e_i differ, too.

7. Fast convolution. The assumptions of section 3 are in force; in particular, the Fourier transform is invertible.

The FFT also induces a fast convolution algorithm for the group algebra $K[G]$ and the polynomial algebra $K[z_1,\cdots,z_r]$. Let, more generally, A be a commmutative K-algebra with a fixed chosen basis of length N, for instance, $K[G]$ with the standard basis. The multiplication $A\times A\to A$ is K-bilinear, but not linear, and therefore requires the notion of a *bilinear or multiplicative* complexity. Several papers and books deal with it and construct fast algorithms of small multiplicative complexity [43], [3], [1], [37], [9, Def. 14.7], [33], [20]. In the present paper we do not treat these algorithms and use only the complexity of linear maps as introduced in section 4. For fixed $a\in A$ the map $A\to A,\ b\mapsto ab$, is K-linear and therefore its linear complexity (with respect to the chosen basis),

$$\mu_A(a):=\mu(A\to A,\ b\mapsto ab)\le N^2\text{ and then }\mu_{\text{lin}}(A):=\max\nolimits_{b\in A}\mu_A(b)\le N^2,\tag{71}$$

is defined according to Definition 46. It is obvious that K^G with the argumentwise multiplication and the standard basis has the complexity

$$\mu_{\mathrm{lin}}(K^G) \le N := \mathrm{ord}(G) \tag{72}$$

since the corresponding matrices are diagonal matrices with at most N nonzero entries.

THEOREM 73 (fast convolution). *The data are as in Theorem* 63. *Let $a \in K[G]$ be an arbitrarily chosen but fixed function and consider the linear map $f : K[G] \to K[G],\ b \mapsto a * b$. Then f is the composition of the maps*

$$f : K[G] \xrightarrow{\mathrm{Four}_G} K^{\widehat{G}} \xrightarrow{\widehat{a}\cdot(-)} K^{\widehat{G}} \xrightarrow{N^{-1}\mathrm{Four}_{\widehat{G}}} K^G \xrightarrow{S_G} K^G,$$

and hence its complexity satisfies

$$\mu_{K[G]}(a) := \mu(f) \le N(1 + 2\Lambda(N)),\ \textit{thus also}\ \mu_{\mathrm{lin}}(K[G]) \le N(1 + 2\Lambda(N)).$$

Proof. Let $c := a * b$; hence $\widehat{c} := \widehat{a}\widehat{b}$ by the convolution theorem. The Fourier inversion theorem implies

$$f(b) = c = S_G(N^{-1}\,\mathrm{Four}_{\widehat{G}})(\widehat{c}) = S_G(N^{-1}\,\mathrm{Four}_{\widehat{G}})(\widehat{a}\widehat{b}),$$

and f is indeed the asserted composition. According to Theorem 49 its complexity is at most the sum of the complexities of its factors. The two Fourier transforms have complexity at most $N\Lambda(N)$ according to Theorem 63 and the argumentwise multiplication with $\widehat{a}$ at most N. The complexity of the antipode is zero since it is an index transformation; see Definition and Corollary 48. The algorithm for $\mathrm{Four}_{\widehat{G}}$ from Theorem 61 can be adapted to the computation of $N^{-1}\,\mathrm{Four}_{\widehat{G}}$ by replacing

$$\widehat{\varphi}_r(k_r, \widehat{k}_r) = \mathrm{fact}_{rr}(k_r, \widehat{k}_r) = \langle k_r, \widehat{k}_r\rangle$$

in the recursion step $c_r \mapsto c_{r-1}$ by $N^{-1}\langle k_r, \widehat{k}_r\rangle$. This implies that also $N^{-1}\,\mathrm{Four}_{\widehat{G}}$ has complexity at most $N\Lambda(N)$, and therefore the complexity of $b \mapsto a * b$ and of $K[G]$ is indeed at most $N(1 + 2\Lambda(N))$. □

ALGORITHM 74 (fast convolution). *The fast algorithm for the convolution $a * b$ in the group algebra $K[G]$ consists of the following steps:*

1. *Precompute the Fourier transform $\widehat{a} \in K^{\widehat{G}}$. This computation and its complexity are not counted because $\widehat{a}$ is assumed known when f is applied.*
2. *Compute $\widehat{b}$ with the decimation in time FFT according to Theorems* 58 *and* 63 *with complexity $N\Lambda(N)$.*
3. *Compute $\widehat{c} := \widehat{a}\widehat{b}$, $(\widehat{a}\widehat{b})(\widehat{g}) = \widehat{a}(\widehat{g})\widehat{b}(\widehat{g})$ with complexity at most N.*
4. *Compute $N^{-1}\widehat{\widehat{c}}$ with the slight modification of the decimation in frequency FFT from Theorem* 61 *with complexity $N\Lambda(N)$ and then apply the antipode to the result to obtain $c = a * b$.*

It suffices to compute $b_r(\widehat{k})$ only in the first FFT-algorithm (see Theorem 58*) and to start the second FFT-algorithm with $c_r(\widehat{k}) = a_r(\widehat{k})b_r(\widehat{k})$; i.e., the computation of the elements $\widehat{g} = \widehat{\mathrm{ind}}(\widehat{k}) = \sum_{j=1}^{r} \lambda_{j-1}^{\star}\widehat{\sigma}_j(\widehat{k}_j)$ is superfluous.*

Remark 75. If in the preceding algorithm for $a * b$ the complexity of computing $\widehat{a}$ is also counted, then the total complexity of the algorithm is $N(1 + 3\Lambda(N))$. Recall, however, that in this article we gave only a formal definition for the complexity of a linear, but not of a bilinear, map like $a * b$ with variable a and b. Our complexity

counts *all* necessary elementary computation steps for the computation of $c = a*b$ and not only the *essential* multiplications which enter into the *multiplicative complexity*.

The fast convolution also induces a fast algorithm for the multiplication of multivariate polynomials in $K[z] = K[z_1, \cdots, z_r]$. For this purpose we consider the case

(73)
$$G = \widehat{G} = \mathbb{Z}/\mathbb{Z}d_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}d_r$$
$$\underset{\text{identification}}{=} I(d) := \{0, \cdots, d_1 - 1\} \times \cdots \times \{0, \cdots, d_r - 1\} \ni \mu = (\mu_1, \cdots, \mu_r),$$
$$\mu \bullet \nu := \overline{\textstyle\sum_{i=1}^{r} \mu_i \nu_i \frac{d}{d_i}} \in \mathbb{Z}/\mathbb{Z}d,\ \langle \mu, \nu \rangle = \zeta^{\mu \bullet \nu}.$$

The group algebra $K[G]$ has the K-basis $\delta_\mu,\ \mu \in G$. With

$$x := (x_1, \cdots, x_r),\ x_i := \delta_{(0, \cdots, 0, 1, 0, \cdots, 0)},\ 1 \text{ at the } i\text{th place},\ i = 1, \ldots, r, \text{ we get}$$
$$\delta_\mu = x^\mu \text{ and } x_i^{d_i} - 1 = 0.$$

Lemma and Definition 76. *The substitution homomorphism $K[z] \to K[G]$, $z_i \mapsto x_i$, induces an isomorphism*

$$K[z]/\langle z_1^{d_1} - 1, \cdots, z_r^{d_r} - 1\rangle \cong K[G],\ \overline{z^\mu} \mapsto \delta_\mu = x^\mu,\ \overline{f} \mapsto f(x). \tag{74}$$

In what follows we therefore identify *these two algebras, i.e., for*

$$f = \textstyle\sum_{\mu \in \mathbb{N}^r} f_\mu z^\mu \in K[z] :\ \overline{f} = f(x) = \sum_{\mu \in \mathbb{N}^r} f_\mu x^\mu = \sum_{\mu \in \mathbb{N}^r} f_\mu \delta_\mu.$$

In particular, we get the K-linear isomorphism

$$K[z]_{I(d)} := \{f \in K[z];\ \textit{for all } i = 1, \ldots, r :\ \deg_{z_i}(f) \le d_i - 1\}$$
$$= \oplus_{\mu \in I(d)} K z^\mu \cong K[G],\ z^\mu \mapsto \delta_\mu = x^\mu.$$

In other words, one can reproduce f from $f(x)$ if the degree bounds $\deg_{z_i}(f) \le d_i - 1$ are observed.

Proof. Induction by means of the canonical isomorphism

$$K[z]/\langle z_1^{d_1} - 1, \cdots, z_r^{d_r} - 1\rangle$$
$$\cong (K[z_1, \cdots, z_{r-1}]/\langle z_1^{d_1} - 1, \cdots, z_{r-1}^{d_{r-1}} - 1\rangle)[z_r]/\langle z_r^{d_r} - 1\rangle$$

shows that this algebra has the K-basis $\overline{z^\mu},\ \mu \in I(d)$. The induced map (74) maps this K-basis onto the basis $x^\mu,\ \mu \in I(d) \underset{\text{ident.}}{=} G$ of $K[G]$, and is thus an isomorphism. ∎

Now let m, n, d be vectors in $\mathbb{N}^r$ with the property

$$m_i + n_i \le d_i + 1,\ i = 1, \ldots, r, \text{ such that } K[z]_{I(m)} \times K[z]_{I(n)} \xrightarrow{\text{mult}} K[z]_{I(d)} \tag{75}$$

is well defined.

Corollary 77 (fast multiplication of polynomials). *The multiplication*

$$K[z]_{I(m)} \times K[z]_{I(n)} \xrightarrow{\text{mult}} K[z]_{I(d)},\ (P, Q) \mapsto PQ,$$
$$P = \textstyle\sum_{\mu \in I(m)} a_\mu z^\mu,\ Q = \sum_{\nu \in I(n)} b_\nu z^\nu, \tag{76}$$
$$PQ = \textstyle\sum_{\lambda \in I(d)} \sum_{\mu, \nu,\ \mu + \nu = \lambda} \{a_\mu b_\nu,\ \mu_j \le m_j - 1,\ \nu_j \le n_j - 1\} z^\lambda$$

equals the composition of the maps

(77)
$$K[z]_{I(m)} \times K[z]_{I(n)} \overset{\text{inj}\times\text{inj}}{\longrightarrow} K[z]_{I(d)} \times K[z]_{I(d)} \cong K[G] \times K[G] \overset{*}{\to} K[G] \cong K[z]_{I(d)}.$$

If the product PQ is computed according to the algorithm in (76)*, the complexity is*

$$\textstyle\prod_{i=1}^{r} m_i n_i.$$

If, on the other hand, (77) *is used with the fast convolution algorithm, Algorithm* 74*, then the algorithm has the complexity*

$$N(1 + 3\Lambda(N)), \text{ where } N = \operatorname{ord}(G) := d_1 * \cdots * d_r.$$

Note that this algorithm depends on the choice of $d_1, \cdots, d_r$.

Proof. The proof is obvious since in (77) all maps except the convolution have complexity zero. See Remark 75 for the applied complexity notion. □

In applications of the preceding algorithm (77) the degrees m_j and n_j are given in general, whereas the numbers $d_j > m_j + n_j - 2$ may be suitably chosen. We illustrate the case

$$r = 1, \quad m_1 = n_1 = m, \quad 2 * (m-1) < d = N.$$

Examples 78.

(1) The standard choice is

$$\begin{gathered} N = 2^e, e \geq 2,\ \Lambda(2^e) = e, m \leq 2^{e-1};\ \text{hence} \\ N(1 + 3\Lambda(N)) = 2^e(1 + 3e).\ \text{But} \\ 2^{e-2} \leq 1 + 3e \text{ for } 2 \leq e \leq 6;\ \text{hence} \\ m^2 \leq 2^{2(e-1)} \leq 2^e(1 + 3e) = N(1 + 3\Lambda(N)) \text{ for } N = 2^e, 2 \leq e \leq 6. \end{gathered}$$

This signifies that for the convolution of polynomials of degree at most 31 the direct computation of complexity $m^2 = 1024$ is faster than the algorithm of (77) with $N = 2^6$ and complexity $2^6 * (1 + 3 * 6) = 1216$.

(2)

$$\begin{gathered} m := 36, N_1 := 72 = 2^3 * 3^2 < N_2 = 128 = 2^7, \\ \Lambda(N_1) = 3 * 1 + 2 * 2 = 7 = \Lambda(N_2).\ \text{Again} \\ m^2 = 1296 < N_1(1 + 3\Lambda(N_1)) = 1584 < N_2(1 + 3\Lambda(N_2) = 2816. \end{gathered}$$

Also in this case the direct computation of the product is better than the two algorithms (77) for N_1 (resp., N_2).

(3)

$$\begin{gathered} m := 70, N_1 = 144 = 2^4 * 3^2, N_2 := 2^8, \\ \Lambda(N_1) = 4 + 2 * 2 = 8 = \Lambda(N_2).\ \text{Then} \\ N_1(1 + 3\Lambda(N_1)) = 3600 < m^2 = 4900 < N_2(1 + 3\Lambda(N_2)) = 6400. \end{gathered}$$

The algorithm for N_1 is faster than the direct computation, while that for the smallest power-of-two, 2^8, which exceeds $2 * 69$ is slower. This example shows that the standard choice of the power-of-two Cooley–Tukey FFT may not work at all or may give bad results for the fast multiplication of polynomials.

(4) This example is a multivariate one with

$$r > 1, \text{ but } m_1 = \cdots = m_r = n_1 = \cdots = n_r = 2.$$

The polynomials P and Q are of degree at most one in each indeterminate z_i or contain only square-free monomials. The direct computation of PQ has the total complexity $\prod_{j=1}^{r} m_j n_j = 4^r$. The optimal choice for the d_j is

$$d_1 = \cdots = d_r = 3; \text{ hence } N = 3^r, \ \Lambda(N) = 2r.$$

The algorithm (77) for these data has the complexity

$$N(1 + 3\Lambda(N)) = 3^r(1 + 6r) < 4^r \text{ for } r \geq 16.$$

The best applicable power-of-two FFT is that with $d_1 = \cdots = d_r = 4$ and the ensuing multiplication complexity $4^r(1 + 6r)$ which is much slower than the direct multiplication.

8. Number theoretic transforms (NTT). The following considerations give interesting examples of the DFT with coefficient rings instead of fields. They are simple variants or special cases of those in [29, Chap. 8], [16], [20, Chap. 7], where also the technical significance of these transforms is discussed. We adapt our notation to that of [29] and consider $N > 0$, a commutative ring K, and a primitive Nth root of one $\zeta \in K$. Consider the groups

$$G := \widehat{G} := \mathbb{Z}/\mathbb{Z}N \underset{\text{ident.}}{=} \{0, \cdots, N-1\} \text{ with } \overline{k} \bullet \overline{l} := \overline{kl} \in \mathbb{Z}/\mathbb{Z}N, \ \langle \overline{k}, \overline{l} \rangle := \zeta^{kl},$$
$$\mu := \langle \zeta \rangle = \{\eta_0, \cdots, \eta_i := \zeta^i, \cdots, \eta_{N-1} := \zeta^{N-1}\}.$$

The Fourier transform $\text{Four} := \text{Four}_G$ on G is given as (see Example 20)

$$a, \ \widehat{a} := \text{Four}_{\mathbb{Z}/\mathbb{Z}N}(a) \in K^N, \ \widehat{a}(l) = \sum_{k=0}^{N-1} \zeta^{lk} a(k), \text{ or}$$
$$\begin{pmatrix} \widehat{a}(0) \\ \widehat{a}(1) \\ \cdots \\ \widehat{a}(N-1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \eta_0 & \eta_1 & \cdots & \eta_{N-1} \\ \cdots & \cdots & \cdots & \cdots \\ \eta_0^{N-1} & \eta_1^{N-1} & \cdots & \eta_{N-1}^{N-1} \end{pmatrix} \begin{pmatrix} a(0) \\ a(1) \\ \cdots \\ a(N-1) \end{pmatrix}.$$

The determinant of this Vandermonde matrix is

$$\det := \prod_{0 \leq i < j \leq N-1} (\eta_j - \eta_i) = \prod_{0 \leq i < j \leq N-1} \zeta^i (\zeta^{j-i} - 1), \tag{78}$$

whose factors are the units ζ^i and the $\eta - 1, \ 1 \neq \eta \in \mu$.

Reminder 79 (see [25, pp. 203–207]). Let $z := \exp(\frac{2\pi i}{N})$ denote a complex primitive Nth root of one and $\nu := \langle z \rangle$ the cyclic group of all complex Nth roots of one. If $d \geq 1$ is a divisor of N, the set $\nu_d := \{z^{\frac{N}{d}k}; 1 \leq k \leq d-1, \gcd(k,d) = 1\}$ consists exactly of the $\varphi(d) := \text{ord}(\text{U}(\mathbb{Z}/\mathbb{Z}d))$ primitive dth roots of one, and the dth *cyclotomic polynomial* $\Phi_d := \prod_{x \in \nu_d} (X - x)$ is the (irreducible) minimal polynomial of all its roots in $\mathbb{Q}[X]$ and has coefficients in $\mathbb{Z}$, the latter property being derived from the obvious product representation

$$X^N - 1 = \prod_{x \in \nu} (X - x) = \prod_{d|N} \prod_{x \in \nu_d} (X - x) = \prod_{d|N} \Phi_d. \tag{79}$$

Since $\Phi_d \in \mathbb{Z}[X]$ the value $\Phi_d(x)$ is defined for every element x of any ring.

THEOREM 80 (see [29, Thms. 8.3, 8.4], [16, Satz 2.8]). *The following assertions are equivalent.*

(1) *Assumption* 29 *is satisfied, and hence the Fourier inversion theorem, Theorem* 34*, holds for all finite abelian groups of exponent* N*, i.e.,* (i) $N \in \mathrm{U}(K)$ *and* (ii)

$$\text{for all } d > 1,\ d \mid N,\ \eta := \zeta^{\frac{N}{d}}: \quad 1 + \eta + \cdots + \eta^{d-1} = 0.$$

(2) *The Fourier transform* $\mathrm{Four}_{\mathbb{Z}/\mathbb{Z}N}$ *is an isomorphism.*

(3) *For all* $\eta \neq 1$ *in* $\mu = \langle\zeta\rangle$ *the element* $\eta - 1$ *is a unit in* K*.*

(4) (i) $N \in \mathrm{U}(K)$. (ii) $\Phi_N(\zeta) = 0$.

Proof. (1) $\Rightarrow$ (2): This is a special case.

(2) $\Leftrightarrow$ (3): The Fourier transform is an isomorphism if and only if its (Vandermonde) determinant (78) is a unit, and this is the case if and only if all factors $\eta - 1,\ 1 \neq \eta \in \mu$, of this determinant are units, the ζ^i being units by assumption.

(3) $\Rightarrow$ (1): As just shown, $\mathrm{Four}_{\mathbb{Z}/\mathbb{Z}N}$ is an isomorphism. Let $d > 1$ be a divisor of N and $\eta := \zeta^{\frac{N}{d}}$ the root of order $\mathrm{ord}(\eta) = d$; hence

$$0 = \eta^d - 1 = (\eta - 1)(\eta^{d-1} + \cdots + 1).$$

But

$$\tfrac{N}{d} < N,\ \mathrm{ord}(\zeta) = N \ \Rightarrow\ \eta \neq 1 \underset{(3)}{\Rightarrow} \eta - 1 \in \mathrm{U}(K) \ \Rightarrow\ \eta^{d-1} + \cdots + 1 = 0,$$

and this is the second condition of Assumption 29. The proof of Theorem 34 then implies that $\mathrm{Four}^2_{\mathbb{Z}/\mathbb{Z}N} = NS_{\mathbb{Z}/\mathbb{Z}N}$. Since $\mathrm{Four}_{\mathbb{Z}/\mathbb{Z}N}$ and $S_{\mathbb{Z}/\mathbb{Z}N}$ are isomorphisms, N is invertible in K.

(1), (2), (3) $\Rightarrow$ (4): Equation (79) implies

$$0 = \zeta^N - 1 = \Phi_N(\zeta) \textstyle\prod_{d|N,\ 1 \leq d < N} \Phi_d(\zeta).$$

But $\Phi_d \mid X^d - 1$ and condition (3) imply that

$$\text{for all } d \text{ with } d \mid N,\ 1 \leq d < N : \Phi_d(\zeta) \in \mathrm{U}(K);$$

hence $\Phi_N(\zeta) = 0$.

(4) $\Rightarrow$ (1): Let $1 < d$ be a divisor of N and let

$$Y := X^{\frac{N}{d}};\ \text{hence } X^N - 1 = Y^d - 1 = (Y - 1)(Y^{d-1} + \cdots + 1).$$

The polynomial Φ_N is irreducible in $\mathbb{Z}[X]$ and divides $X^N - 1$, but not $X^{\frac{N}{d}} - 1$ since $d > 1$; hence Φ_N divides $Y^{d-1} + \cdots + 1$. But then

$$\Phi_N(\zeta) = 0,\ \eta := Y(\zeta) = \zeta^{\frac{N}{d}},\ \text{and thus } \eta^{d-1} + \cdots + 1 = 0.$$

This is exactly the second condition of Assumption 29. □

Reminder 81 (see [25, Exercise 7, p. 73]). Let

$$p = \text{odd prime},\ m \geq 1,\ K := \mathbb{Z}/\mathbb{Z}p^m,\ \mathrm{can} : K \to \mathbb{Z}/\mathbb{Z}p,\ \overline{k} \mapsto \overline{k}. \text{ The group}$$
$$\mathrm{U}(K) = \{\eta = \overline{k} \in K;\ \gcd(p, k) = 1 \text{ or } \mathrm{can}(\eta) \neq 0 \text{ or } \mathrm{can}(\eta) \in \mathrm{U}(\mathbb{Z}/\mathbb{Z}p)\}$$

is cyclic of order $\varphi(p^m) = p^{m-1}(p-1)$. More precisely, one obtains an exact sequence

$$1 \to \langle 1 + \overline{p}\rangle \xrightarrow{\subseteq} \mathrm{U}(K) \underset{\sigma}{\overset{\mathrm{can}}{\rightleftarrows}} \mathrm{U}(\mathbb{Z}/\mathbb{Z}p) \to 1,$$

where $\langle 1+\overline{p}\rangle$ is cyclic of order p^{m-1} and where σ is the unique section of can which satisfies the condition $\sigma(\lambda^p) = \sigma(\lambda)^p$; indeed, σ is the well-defined map

$$\sigma : \mathrm{U}(\mathbb{Z}/\mathbb{Z}p) \to U(K),\ \overline{k} \mapsto \overline{k^{p^{m-1}}},$$

is a monomorphism and induces the isomorphism

$$\mathrm{U}(\mathbb{Z}/\mathbb{Z}p) \times \langle 1+\overline{p}\rangle \cong \mathrm{U}(K),\ (\lambda, \eta) \mapsto \sigma(\lambda)\eta.$$

Since $\mathrm{U}(\mathbb{Z}/\mathbb{Z}p)$ is cyclic of order $p-1$ and $\gcd(p^{m-1}, p-1) = 1$, the Chinese remainder theorem implies that $\mathrm{U}(K)$ is cyclic, too, and is generated by $\sigma(\lambda)(1+\overline{p})$, where λ is a primitive $(p-1)$st root of one in $\mathbb{Z}/\mathbb{Z}p$. If $p = 2$ and $m \geq 3$, the group $\mathrm{U}(\mathbb{Z}/\mathbb{Z}2^m)$ is not cyclic and is uninteresting for the DFT as will be shown instantly.

LEMMA 82. *Let p be prime, $m \geq 1$, $K := \mathbb{Z}/\mathbb{Z}p^m$, and $\zeta \in K$ a primitive Nth root of one which satisfies the equivalent conditions of Theorem* 80. *Then N divides $p-1$. In particular, if $p = 2$, then $N = 1$ and $\zeta = 1$, and therefore the case $p = 2$ is uninteresting in context with the DFT.*

Proof. Assume $p - 1 < N$. By Theorem 80, $\zeta^{p-1} - 1$ is a unit in K and hence so is $\mathrm{can}(\zeta^{p-1} - 1) = \mathrm{can}(\zeta)^{p-1} - 1 = 0$ in $\mathbb{Z}/\mathbb{Z}p$, which is a contradiction. On the other hand, N divides the order $\varphi(p^m) = p^{m-1}(p-1)$ of $\mathrm{U}(K)$, and thus N is a divisor of $p-1$. □

THEOREM 83 (see [29, Thm. 8.6], [16, Satz 2.2]). *Let $M > 2$ be an odd number, $M = p_1^{m_1} * \cdots * p_s^{m_s}$ its prime factor decomposition, $K = \mathbb{Z}/\mathbb{Z}M$, and $N > 0$. Then K contains an Nth root of one satisfying the equivalent conditions of Theorem* 80 *if and only if N divides* $\gcd(p_1 - 1, \cdots, p_s - 1)$.

Proof. The Chinese remainder theorem furnishes the isomorphism

$$\Delta : K = \mathbb{Z}/\mathbb{Z}M \cong K_1 \times \cdots \times K_s := \mathbb{Z}/\mathbb{Z}p_1^{m_1} \times \cdots \times \mathbb{Z}/\mathbb{Z}p_s^{m_s},\ \overline{k} \mapsto \Delta(\overline{k}) = (\overline{k}, \cdots, \overline{k}).$$

Assume $\zeta \in K$ satisfies the assumptions of Theorem 80 and let

$$\Delta(\zeta) = (\zeta_1, \cdots, \zeta_s);\ \text{hence } N = \mathrm{ord}(\zeta) = \mathrm{lcm}(N_1, \cdots, N_s),\ N_i := \mathrm{ord}(\zeta_i),\ \text{and}$$
$$\Delta(\zeta^m - 1) = (\zeta_1^m - 1, \cdots, \zeta_s^m - 1).$$

The latter element is a unit if $m := N_i < N$, but $\zeta_i^{N_i} - 1 = 0$; hence $N = N_1 = \cdots = N_s$ and $N \mid p_i - 1,\ i = 1, \ldots, s$, by Lemma 82.

If, conversely, this is the case, if λ_i is a generator of $\mathrm{U}(\mathbb{Z}/\mathbb{Z}p_i)$ and if $\sigma_i : \mathrm{U}(\mathbb{Z}/\mathbb{Z}p_i) \to \mathrm{U}(\mathrm{K}_i)$ is the section according to Reminder 81, then

$$\zeta := \Delta^{-1}\left(\sigma_1\left(\lambda_1^{\frac{p_1-1}{N}}\right), \cdots, \sigma_s\left(\lambda_1^{\frac{p_s-1}{N}}\right)\right)$$

is the asserted root of one. □

We refer the reader to [29] and [20] for the discussion of special cases of the preceding theorem, in particular, those of *Mersenne and Fermat number transforms* with $M = 2^n - 1$ (resp., $M = 2^n + 1$).

Acknowledgment. I thank the two referees for their careful reading of the article, their positive opinion, and their suggestions. These have been incorporated into the revised version to the best of my abilities. One of the referees is obviously an aesthete.

REFERENCES

[1] L. Auslander, E. Feig, and S. Winograd, *The multiplicative complexity of the discrete Fourier transform*, Adv. in Appl. Math., 5 (1984), pp. 31–55.

[2] L. Auslander and R. Tolimieri, *Is computing with the finite Fourier transform pure or applied mathematics?*, Bull. Amer. Math. Soc. (N.S.), 1 (1979), pp. 847–897.

[3] L. Auslander and S. Winograd, *The multiplicative complexity of certain semilinear systems defined by polynomials*, Adv. in Appl. Math., 1 (1980), pp. 257–299.

[4] K. G. Beauchamp, *Transforms for Engineers. A Guide to Signal Processing*, Clarendon Press, Oxford, UK, 1987.

[5] T. Beth, *Verfahren der schnellen Fouriertransformation*, Teubner, Stuttgart, Germany, 1984.

[6] N. Bourbaki, Éléments de mathé matique. Fasc. XXXII: *Théories spectrales*, Hermann, Paris, 1967, chap. I–II.

[7] W. L. Briggs and V. E. Henson, *The DFT*: An Owners' Manual for the Discrete Fourier Transform, SIAM, Philadelphia, 1995.

[8] E. O. Brigham, *The Fast Fourier Transform*, Prentice–Hall, Englewood Cliffs, NJ, 1974.

[9] P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic Complexity Theory*, Springer, Berlin, 1997.

[10] C. S. Burrus, *Efficient Fourier transform and convolution algorithms*, in Advanced Topics in Signal Processing, J. S. Lim and A. V. Oppenheim, eds., Prentice–Hall, Englewood Cliffs, NJ, 1988, pp. 199–245.

[11] C. S. Burrus, et al., *Computer-Based Exercises for Signal Processing Using MATLAB*, Prentice–Hall, Englewood Cliffs, NJ, 1994.

[12] J. S. Byrnes, ed., *Twentieth Century Harmonic Analysis—A Celebration*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2001.

[13] M. Clausen and U. Baum, *Fast Fourier Transforms*, BI-Wissenschaftsverlag, Mannheim, Germany, 1993.

[14] E. Chu and A. George, *Inside the FFT Black Box*, CRC Press, Boca Raton, FL, 2000.

[15] C. K. Chui and G. Chen, *Signal Processing and Systems Theory*, Springer, Berlin, 1992.

[16] R. Creutzburg and M. Tasche, *F-Transformation und Faltung in kommutativen Ringen*, Elektron. Inform.-Verarb. Kybernetik, 21 (1985), pp. 129–149.

[17] R. Creutzburg and M. Tasche, *Number-theoretic transforms of prescribed length*, Math. Comp., 47 (1986), pp. 693–701.

[18] J. C. Cooley and J. C. Tukey, *An algorithm for machine calculation of complex Fourier series*, Math. Comp., 19 (1965), pp. 297–301.

[19] D. E. Dudgeon and R. M. Mersereau, *Multidimensional Digital Signal Processing*, Prentice–Hall, Englewood Cliffs, NJ, 1984.

[20] H. K. Garg, *Digital Signal Processing Algorithms*, CRC Press, Boca Raton, FL, 2000.

[21] I. J. Good, *The relationship between two fast Fourier transforms*, IEEE Trans. Comput., 20 (1971), pp. 310–317.

[22] L. Hörmander, *The Analysis of Linear Partial Differential Operators* I, Springer, Berlin, 1983.

[23] E. Kamen, *Introduction to Signals and Systems*, Macmillan, New York, 1987.

[24] V. P. Khavin, *Methods and structure of commutative harmonic analysis* I, in Commutative Harmonic Analysis, Encyclopaedia Math. Sci., 15, V. P. Khavin and N. K. Nikol'skij, eds., Springer, Berlin, 1991, pp. 1–111.

[25] S. Lang, *Algebra*, Addison–Wesley, Reading, MA, 1965.

[26] J. S. Lim, *Two-dimensional signal processing*, in Advanced Topics in Signal Processing, J. S. Lim and A. V. Oppenheim, eds., Prentice–Hall, Englewood Cliffs, 1988, pp. 338–415.

[27] J. S. Lim and A. V. Oppenheim, eds., *Advanced Topics in Signal Processing*, Prentice–Hall, Englewood Cliffs, NJ, 1988.

[28] H. D. Lüke, *Signalübertragung*, Springer, Berlin, 1990.

[29] H. J. Nussbaumer, *Fast Fourier Transform and Convolution Algorithms*, Springer, Berlin, 1981.

[30] U. Oberst, *Explizite Rekursionsformeln zur schnellen Fouriertransformation*, Actes Sémi. Loth. de Combinatoire, 18 (1988), pp. 119–126, Publ. IRMA, Strasbourg.

[31] U. Oberst, *The Fast Fourier Transform*, Publ. 79, Centro Vito Volterra, Universita di Roma II, 1991.

[32] U. Oberst, *Galois Theory and the Fast Gelfand Transform*, Publ. 99, Centro Vito Volterra, Universita di Roma II, 1992.

[33] U. Oberst and S. Walch, *The Optimal Fast Fourier, Gelfand and Hartley Transforms*, in preparation.

[34] A. V. Oppenheim and R. W. Schafer, *Discrete-Time Signal Processing*, Prentice–Hall, Englewood Cliffs, NJ, 1989.

[35] A. V. Oppenheim and A. S. Willsky, *Signals and Systems*, Prentice–Hall, Englewood Cliffs, NJ, 1983.
[36] C. M. Rader, *Discrete Fourier transforms when the number of data points is prime*, Proc. IEEE, 56 (1968), pp. 1107–1108.
[37] V. Strassen, *Algebraic complexity theory*, in Algorithms and Complexity, J. V. Leeuwen, ed., Elsevier, Amsterdam, 1990, pp. 633–672.
[38] R. Tolimieri, *Multiplicative characters and the discrete Fourier transform*, Adv. in Appl. Math., 7 (1986), pp. 344–380.
[39] R. Tolimieri and M. An, *Lesser known FFT algorithms*, in Twentieth Century Harmonic Analysis—A Celebration, J. S. Byrnes, ed., Kluwer Academic Publishers, Dordrecht, The Netherlands, 2001, pp. 151–162.
[40] R. Unbehauen, *Systemtheorie*, Oldenbourg Verlag, München, Germany, 1990.
[41] S. Walch, *Schnelle äquivariante Gelfand- und Fouriertransformationen*, Dissertation, Innsbruck, 1994.
[42] S. Winograd, *On computing the discrete Fourier transform*, Math. Comp., 32 (1978), pp. 175–199.
[43] S. Winograd, *On the multiplicative complexity of the discrete Fourier transform*, Adv. in Math., 32 (1979), pp. 83–117.