SVEN BODO WIRSING

ON UNIT GROUPS OF MODULAR GROUP ALGEBRAS

The concept of end-commutable ordering - with 241 exercises

Anchor Academic Publishing
disseminate knowledge

Wirsing, Sven Bodo: On unit groups of modular group algebras.
The concept of end-commutable ordering – with 241 exercises,
Hamburg, Anchor Academic Publishing 2019

Buch-ISBN: 978-3-96067-224-1
PDF-eBook-ISBN: 978-3-96067-724-6
Druck/Herstellung: Anchor Academic Publishing, Hamburg, 2019

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Bibliographical Information of the German National Library:
The German National Library lists this publication in the German National Bibliography. Detailed bibliographic data can be found at: http://dnb.d-nb.de

Hermannstal 119k, 22119 Hamburg
https://www.anchor-publishing.com, Hamburg 2019
Printed in Germany

Contents

For Pia, Jan and Emily

Prime factors

My heart, it holds a secret prime,
and your heart holds one, too.
I ask you now, will you join hearts,
and multiply them through?
We will make a product so sublime
it overtakes the skies
and stay together all our days
till death us factorize.

(unknown author, see [81])

The theory of groups is a central discipline within the algebra. Not only specific group theoretical methods but also concepts of other disciplines are used to analyze groups. The representation and the character theory of finite groups are two prominent examples of these methods. The exact study of the group algebra is an effectual source of insights for modules and characters. Therefor, the analysis of the group algebra has a long tradition within the theory of associative algebras (S. Jennings [30], 1941 and D.S. Passman [51], 1977). Whether the group algebra over a field K is semisimple or modular is – based on the theorem of Maschke – identifiable at the characteristic of K. Within this work the group of units of the group algebra is analyzed for a p-group and a field of characteristic p.

The structure of the group of units of the group algebra for an Abelian p-group and a finite field of characteristic p is analyzed by R. Sandling in [57], by A. Albrecht in [1] and by A. Bovdi and A. Szakacs in [13]. One main topic of this work is to determine the structure of the center of the group of units $E(KG) = (1_G + rad(KG)) \times (K \setminus \{0_K\}) \cdot 1_G$ of the group algebra KG for an non-Abelian p-group G and a field K of characteristic p.

We generalize a result of K.R. Pearson [53] at the beginning of the first chapter: for an arbitrary subgroup U of G the set $Z(G) \cap U$ is the core of U in $1_G + rad(KG)$ (corollary 1.2.3). The normalizer of U in $1_G + rad(KG)$ is determined by $N_G(U) \cdot C_{1_G + rad(KG)}(U)$ which is proven afterwards (theorem 1.3.6). The special case $U = G$ is contained in the article of D.B. Coleman (see [19]). His concept of fixed points is analyzed and generalized.

Our concept of analyzing the center of $E(KG)$ is developed within this work and is called end-commutable ordering of algebra-elements. This method is presented within the second chapter of this work. We prove (see theorem 2.3.6) that every finite group G is nilpotent if and only if every conjugacy class of G is end-commutable. In addition, we can obtain within theorem 2.1.5 for end-commutable K-algebra elements $a_1, \ldots, a_n$ the important identity $(\sum_{i=1}^{n} a_i)^{p^r} = \sum_{i=1}^{n} a_i^{p^r}$ $(p = char(K), r \in \mathbb{N})$. In the – also for our analysis – important case that $\{a_1, \ldots, a_n\}$ is a conjugacy class of a p-group also A.A. Bovdi and Z. Patay have proven this statement in [9] based on a different argumentation. We apply our method for determining the exponent of $Z(1_G + rad(KG))$ – which was also done by the same authors – purely based on characteristics of the underlying group G (theorem 2.4.8). We finalize chapter 2 by presenting some bounds for this exponent in preparation of chapter 3.

The value $\frac{|G|}{p^2}$ is the maximal possible one for the exponent of $Z(1_G + rad(KG))$ in the case of a non-Abelian p-group G (corollary 2.5.3). Within section 1 of chapter 3 we determine those groups for which this value occur: either the center of G is cyclic of order $\frac{|G|}{p^2}$ or G possesses a cyclic maximal subgroup (theorem 3.1.6).
Groups for which the center of $1_G + rad(KG)$ is elementary-Abelian are characterized in section 2 of chapter 3: the center of G is elementary-Abelian and for all $g \in G \setminus Z(G)$ the identity $C_G(g) < C_G(g^p)$ is valid (theorem 3.2.1). For example, the p-Sylow subgroups of $GL(n, GF(p^k))$ are of this kind (corollary 3.2.2.6).
In diverse interesting cases the exponent of $Z(1_G + rad(KG))$ is identical to the one of $Z(G)$: we prove this for p-groups G for which the identity $exp(G/Z(G)) \leq exp(Z(G))$ is valid (theorem 3.3.1) and – by using a complete different argument – for regular p-groups (corollary 3.3.3).
In the following sections of this chapter we analyze the exponent for group constructions. For central products of two p-groups G, H we obtain the same exponent as for their direct product which is
$max\{exp(Z(1_G + rad(KG))), exp(Z(1_G + rad(KH)))\}$ (theorem 3.4.7).
We proceed the analysis by determining the exponent for an arbitrary wreath product $G \wr_\delta H$: the exponent can be calculated based on the ingredients G, H and δ (theorem 3.5.11). As a consequence, we can bound the exponent for an arbitrary action δ by the lower bound $exp(Z(1_G + rad(KG)))$ and by the upper bound $exp(Z(1_{G\times H} + rad(G \times H)))$ (corollary 3.5.18). The lower value is valid for a faithful (corollary 3.5.16) and the upper bound for the trivial action (remark 3.5.17).
For dihedral, semi-dihedral and quaternion groups of the same order the exponent of the center of $1_G + rad(KG)$ is identical. We generalize this results to two group extensions by Abelian p-groups with equivalent action and a special additional characteristic (theorem 3.6.6).

The concept of end-commutable orderings allows us not only to determine the exponent of $Z(1_G + rad(KG))$ but also the description of the p-power structure of $Z(1_G + rad(KG))$ and henceforth – for a finite field – to calculate the invariants of this Abelian p-group. We can reduce the problem to the direct factor $1_G+rad(KZ(G))$ and its co-factor $1_G+\langle\{\sum_{x\in g^G} x \mid g \in G\backslash Z(G)\}\rangle_K$ of the center of $1_G + rad(KG)$ related to the conjugacy class sums (corollary 4.1.5). The invariants of the first factor are – as already mentioned for Abelian group algebras – completely known, and the ones of the second factor are described in two different ways (by using the chain of Frattini subgroups and the chain of socles) only by using the field K and the group G (theorem 4.3.1.3, theorem 4.3.2.6). Another description is included in the analysis of A. Bovdi and Z. Patay in [10]. The determination of the invariants and the exponent is described by using a special graph: the class-graph. The class-graph visualizes the p-power structure of the co-factor $1_G + \langle\{\sum_{x\in g^G} x \mid g \in G \setminus Z(G)\}\rangle_K$. The exponent of the co-factor is related to the longest path within this graph, the invariants can be calculated by counting the number of special paths within it. Groups with isomorphic class-graphs possess isomorphic co-factors. We determine the invariants for some examples: we prove that the centers of $1_G + rad(KG)$ for quaternion, dihedral and semi-dihedral groups of the same order over a finite field of characteristic 2 are isomorphic (example 4.5.2.2). The last section is dedicated to isoclinic groups. We prove that the exponents of the co-factors of the center of the radicals of two isoclinic groups are identical. We use the result to describe the structure of the center of the radical for semi extra-special groups, ultra-special groups, VZ-groups, Camina and generalized Camina groups.

In chapter 5 of this work we prove at first that the derived subgroup of $1_G + rad(KG)$ is cyclic only for Abelian G (theorem 5.1.4). Afterwards we prove that $(1_G + rad(KG))^p$ is cyclic if and only if G is elementary-Abelian or G is Abelian and $p = \mid G^2 \mid = \mid K^2 \mid = 2$ is valid (corollary 5.2.11).
The group $1_G + rad(KG)$ is special only for an extra-special 2-group G (proposition 5.3.9). For such a group G the elementary-Abelian center of $1_G + rad(KG)$ is identical to the Frattini subgroup of $1_G + rad(KG)$ and contains all squares (lemma 5.3.2, theorem 5.3.3). Within this work we do not give a description of all groups G such that $1_G + rad(KG)$ is a special 2-group. But in the smallest relevant case we prove that the derived subgroup of $1_G + rad(KG)$ is of index 2 in $Z(1_G + rad(KG))$ (example 5.3.10).

Within chapter 6 we focus on the chain of iterated p-groups defined by $G_0 := G$ and $G_{n+1} := 1 + rad(KG_n)$ for all $n \in \mathbb{N}$ over a finite field K of characteristic p and a non-Abelian p-group G. The previous chapters are linked to $G_1 = 1 + rad(KG)$. Now we want to study the behavior of this chain. Several parameters of this chain turn out to be increasing resp. unbounded (see proposition 6.1.2, e.g. the corresponding chain of derived subgroups, of breadth, of nilpotency classes, of strong derived length, of class numbers, of Baer-length). As a consequence the corresponding chain of degrees of commutativities converges against zero.

But the structure of the centers related to this chain can be described differently: the exponents are stable after the second step because the direct factor related to the class sums is elementary-p-Abelian. This result is generalized to arbitrary radical algebras (see theorem 6.2.11 and corollary 6.2.12). As a consequence we can prove that the chain of corresponding exponents and the chain of Engel-length of $(G_n)_{n\in\mathbb{N}_0}$ are unbounded (see theorem 6.3.3).

Some applications are also transferred to the exercises at the end of each chapter. Some exercises are included enhancing the theory presented so far. In addition, at the beginning of each exercise series some open-ended topics are included which can be used by the reader – and also by the author – to do additional researches within this theory. The author has included some graphics – mostly so called Hasse diagrams – to visualize the main results of this work.

The author has prepared some slides which can be used as a basic for a presentation of this work. These slides are available and can be requested at the Anchor Academic Publishing service by using the email address info@anchor-publishing.com.

List of symbols

In this chapter we list all symbols used in this work, present a short description and link (section and page) the first appearance of the symbol within this work.

Chapter 1

$*$	the star composition; 1.1.1, 11
$cl(A)$	class of nilpotency of an associative algebra; exercise 27, 33
$Q(A)$, A^*	the group of units of the monoid $(A;*)$; 1.1.3, 11
a'	the inverse of $a \in Q(A)$; 1.1.3, 11
$E(A)$	the group of units of an associative unitary algebra A; 1.1.3, 11
(I,T)	a semidirect decomposition of an algebra; 1.1.6, 12
(N,U)	a semidirect decomposition of a group; 1.1.6, 12
$S+T$	$:= \{s+t \mid (s;t) \in S \times T\}$; 1.1.8, 13
$s+T$	$:= \{s\} + T$; 1.1.8, 13
$\overline{M}$	$:= \sum\limits_{m \in M} m$; 1.1.9, 13
n_K	$:= \sum\limits_{i=1}^{n} 1_K$; 1.1.9, 13
$\mid T \mid$	the order of a finite set T; 1.1.9, 13
e_H	$:= \frac{1}{\lvert H \rvert}\overline{H}$; 1.1.9, 13
KM	the free K-module with K-basis M ; 1.1.9, 13
$Z(A)$	the center of an algebra A; 1.1.10, 13
$\cong_K$	the isomorphism within the class of K-spaces; 1.1.11, 14
$\langle \ldots \rangle_K$	the K-span within a K-space; 1.1.11, 14
$\mathcal{A}$	the class of associative algebras; 1.1.11, 14
$\mathcal{A}_1$	the class of associative unitary algebras; 1.1.11, 14
$\mathcal{L}$	the class of Lie algebras; 1.1.11, 14
$\mathcal{G}$	the class of groups; 1.1.11, 14
$\cong_{\mathcal{K}}$	the isomorphism within the class $\mathcal{K}$; 1.1.11, 14
$\langle \ldots \rangle_{\mathcal{K}}$	the span within the class $\mathcal{K}$; 1.1.11, 14
$\mathbb{N}$	the set of natural numbers; 1.1.11, 14
$\mathbb{H}$	the set of real quaternions; exercise 9, 31
$\underline{n}$	$:= \mathbb{N}_{\leq n}$; 1.1.11, 14

$\underline{n}_0$	$:= \underline{n} \cup \{0\}$; 1.1.11, 14
$Aug_B(V)$	$:= \langle \{b_1 - b_2 \mid b_1, b_2 \in B\} \rangle_K$; 1.1.12, 14
$aug_B(\sum_{b \in B} k_b b)$	$:= \sum_{b \in B} k_b$; 1.1.12, 14
$Aug(KM)$	$:= Aug_M(KM)$; 1.1.12, 14
$aug(x)$	$:= aug_M(x)$, $x \in KM$; 1.1.12, 14
aug	the augmentation function; 1.1.13, 14
$ker\, \alpha$	the kernel of the function α; 1.1.13, 14
G/N	the factor group of G modulo N; 1.1.14, 14
Ng	an element of G/N; 1.1.14, 14
p_N	the linearization of $g \mapsto Ng$; 1.1.14, 14
$T \cdot S$	$:= \langle \{ts \mid (t, s) \in T \times S\} \rangle_K$; 1.1.14, 14
$rad(A)$	the nilradical of an associative algebra A; 1.1.15, 17
$o(g)$	the order of an element g of a group; 1.1.15, 17
$Z(G)$	the center of the group G; 1.1.15, 17
$char(K)$	the characteristic of the field K; 1.1.15, 17
Q_n	the quaternion group of order n; 1.1.19, 19
$core_G(U)$	the core of U in G; 1.2.1, 20
g^h	$:= h^{-1}gh$; 1.2.2, 20
T^h	$:= \{t^h \mid t \in T\}$; 1.2.2, 20
$Abb(M, N)$	the set of functions between M and N; 1.3.1, 23
$\overline{\delta}$	the linearization of δ; 1.3.3, 23
$\hat{\delta}$	enhanced group action with respect to δ; 1.3.3, 23
$\alpha_{\vert T}$	the restriction of α to T; 1.3.2, 23
$N_G(U)$	the normalizer of U in G; 1.3.6, 24
$C_G(U)$	the centralizer of U in G; 1.3.6, 24
$[g, h]$	the commutator of g and h; 1.3.10, 27
$c(G)$	the class number of G; 1.3.10, 27
$U \oplus_K W$	the inner direct sum of the K-subspaces U and W; 1.3.11, 27
$dim_K(V)$	the dimension of the K-space V; 1.3.11, 27
$C_{KM,\delta}(U)$	the centralizer of U in KM with respect to δ; 1.3.13, 29
κ_g	the conjugation with g; 1.3.15, 29
κ	the function $g \mapsto \kappa_g$; 1.3.15, 29
g^G	the conjugacy class of g in G; 1.3.11, 27

Chapter 2

$EA(T)$	the set of end-commutable orderings of a set T; 2.1.1, 37
S_n	the symmetric group on $\underline{n}$; 2.1.2, 37
D_n	the dihedral group of order n; 2.1.2, 37
$C_A(T)$	the centralizer of T in A; 2.1.5, 38
$Aut(G)$	the group of automorphism of G; 2.1.8, 40
$Stab_G(m)$	the stabilizer of m in G; 2.1.8, 40
$Inn(G)$	the group of inner automorphism of G; 2.1.9, 41

V_4	the Klein four-group; 2.1.9, 41
$G^{'}$	the derived subgroup of G; 2.2.1, 44
$\Phi(G)$	the Frattini subgroup of G; 2.2.1, 44
$F(G)$	the Fitting subgroup of G; 2.3.4, 48
$\mathbb{C}$	the complex number field; 2.3.8, 50
φ_T	the monotone bijection between $\mid T \mid$ and T; 2.4.1, 52
$\binom{T}{i}$	the set of subsets of order i of T; 2.4.2, 52
$\mathbb{N}_0$	$:= \mathbb{N} \cup \{0\}$; 2.4.2, 52
$\binom{n}{i}$	$:=\mid \binom{\underline{n}}{i} \mid$; 2.4.4, 53
G^n	$:= \langle \{g^n \mid g \in G\} \rangle_{\mathcal{G}}$; 2.4.5, 53
K^{p^n}	$:= \{k^{p^n} \mid k \in K\}$, K a field; 2.4.5, 53
$exp(G)$	the exponent of a torsion group G; 2.4.5, 53
$max\,T$	the maximum of a finite subset T of $\mathbb{N}$; 2.4.7, 54
$min\,T$	the minimum of a finite subset T of $\mathbb{N}$; 2.4.8, 55
$C_G(g)$	$:= C_G(\{g\})$; 2.4.8, 55
$a \circ b$	$:= ab - ba$; 2.4.9, 56
A°	the associated Lie algebra of A; 2.4.9, 56
$\mathcal{K}(G)$	the set of conjugacy classes of G; 2.5.1, 57
$gcd(a,b)$	greatest common divisor of a, b; exercise 46, 63

Chapter 3

SD_n	the semi dihedral group of order n; 3.1.2, 67
Z_n	the cyclic group of order n; 3.1.6, 69
$GL(n,K)$	the general linear group; 3.2.2.1, 71
$GF(p^k)$	the finite field with p^k elements; 3.2.2.1, 71
P_n	a p-Sylow subgroup of $GL(n, GF(p^k))$; 3.2.2.1, 71
$K^{n \times n}$	$:= K^{\underline{n} \times \underline{n}}$; 3.2.2.1, 71
$E_{i,j}$	a basis vector of $K^{n \times n}$; 3.2.2.2, 71
$su(n,K)$	strict lower triangular matrices of $K^{n \times n}$; 3.2.2.2, 71
$PGL(n,K)$	the projective linear group; 3.2.2.6, 72
$SL(n,K)$	the special linear group; 3.2.2.6, 72
$PSL(n,K)$	the projective special linear group; 3.2.2.6, 72
$G \times H$	the direct product of two groups G, H; 3.4.1, 76
D_μ, D	$:= \{(u; (u\mu)^{-1}) \mid u \in U_1\}$; 3.4.1, 76
$G_1 \curlyvee_\mu G_2, G_1 \curlyvee G_2$	the central product of two groups G, H; 3.4.1, 76
A^B	$:= Abb(B,A)$; 3.4.9, 79
$a \equiv b \, mod \, c$	c divides $a - b$; 3.4.11, 79
φ^s, $\tilde{s}$	two special functions; 3.5.1, 81
$H \wr_\delta S$, $H \wr_X S$	the wreath product of two groups G, H; 3.5.2, 81
$H \wr S$	the regular wreath product of H with S; 3.5.2, 81
$\alpha \equiv h$	the constant function with value h; 3.5.4, 81
$G/_r U$	the set of right cosets of U in G; 3.5.6, 82
$[A,B]$	$:= \langle \{[a,b] \mid a \in A, b \in B\} \rangle_{\mathcal{G}}$; 3.5.7, 83

$Fix_X(g)$ $:= \{x \mid x \in X, xg = x\}$; 3.5.7, 83
α_h the constant function with unique value h; 3.5.9, 84
$C(2n, q)$ the symplectic group; 3.5.15, 87
$U(n, q^2)$ the unitary group; 3.5.15, 87
$O_D(n, q)$ the orthogonal group; 3.5.15, 87
$(H \times N; \cdot_{\alpha, N(\cdot;\cdot)})$ the group extension of G by N; 3.6.2, 90
$N_R(\cdot\,;\cdot)$ the factor system for the representive system R; 3.6.1, 89
$\alpha_R(h)$ the automorphism for the representive system R; 3.6.1, 89

Chapter 4

$\overline{\mathcal{K}(G)}$ $:= \langle\{\overline{g^G} \mid g \in G \setminus Z(G)\}\rangle_K$; 4.1.6, 103
nG another symbol for $G^{\underline{n}}$; 4.2.1.1, 104
$\overline{k(G)}_{p^i}$ the dimension of $(\overline{\mathcal{K}(G)}^*)^{p^i}$; 4.3.1.2, 109
$soc_n(G)$ the n-th socle of G; 4.3.2.1, 110
$\sim_n$ a special equivalence relation on $\mathcal{K}(G) \setminus \{\{z\} \mid z \in Z(G)\}$; 4.3.2.4, 111
log logarithm; exercise 135, 123
$[,]_G$ the commutator map of a group G; 4.6.2, 119

Chapter 5

A^n $:= \langle\{a_1 \dots a_n \mid a_i \in A\}\rangle_K$; 5.1.2, 133
$a_1 \circ \cdots \circ a_n$ $:= (\dots(a_1 \circ a_2) \circ \dots) \circ a_n$; 5.2.1, 137
$cl(G)$ the class of nilpotency for a nilpotent group G; 5.2.2, 137
$cl(L)$ the class of nilpotency for a nilpotent Lie algebra L; 5.2.2, 137
$Z_n(G)$ the n-th center of a group G; before 5.2.5, before 139
$Z_n(L)$ the n-th center of a Lie algebra L; before 5.2.5, before 139
$L \circ L$ $:= \langle\{a \circ b \mid a, b \in L\}\rangle_K$; 5.2.6, 140
U_{even} a special subgroup of $E(KG)$; 5.3.7, 147

Chapter 6

$J(A)$ Jacobson radical of an algebra A; 6.2.5, 165
$L^{(n)}$ n-th term of the lower central chain of a Lie algebra L; 6.2.5, 165
$a^{(b)}$ star conjugate of a with b; 6.2.5, 165
$ad(a)$ right multiplication with a in a Lie algebra; 6.2.10, 168
$b(G)$ breadth of a group G; 6.1.2, before 160
$st(A)$ solvable class or derived length of an algebra A; 6.1.2, before 160
$(G_n)_{n\in\mathbb{N}_0}$ a special chain of p-groups; 6.1.1, 159
W_n n-th term of a special upper central chain; 6.2.5, 165
X_n n-th term of a special upper central chain; 6.2.5, 165
$\gamma_n(G)$ n-th term of the lower central chain of G; 6.2.5, 165
$d(G)$ degree of commutativity of G; 6.1.2, 160

Chapter 1

Cores and normalizers

1.1 A first reduction

Within this work a K-algebra is an algebra defined based on a commutative unitary ring K.

1.1.1 Definition (star composition)

Let A be a K-algebra. For all $a, b \in A$ we define

$$a * b := a + b + ab.$$

B.L. van der Waerden calls $*$ the star composition on A.$\diamond$

1.1.2 Remark ($\star$ versus $\cdot$)

For every associative K-algebra A the following statements are valid:

(i) $(A; *)$ is a monoid possessing the unit element 0_A.

(ii) If A is unitary, then the function $A \to A$, $a \mapsto 1_A + a$ is a monoid isomorphism between $(A; *)$ and $(A; \cdot)$.$\diamond$

1.1.3 Definition (star group)

If A is an associative K-algebra, then we denote by $Q(A)$ the group of units of the monoid $(A; *)$ and for every $a \in Q(A)$ by a' the inverse of a in $Q(A)$. The elements of $Q(A)$ are called star regular or quasi regular and the group $Q(A)$ is called the star or quasi regular group of A. If A is unitary, then $E(A)$ is called the group of units of A.$\diamond$

The following remark shows us that the star group is a generalization of the group of units in the context of non-unitary associative algebras.

1.1.4 Remark

For every K-algebra A the following statements are valid:

(i) For all $a, b, c, d \in A$ the identity $(a+b)*(c+d) = a*c+b*d+ad+bc$ is true.

(ii) If A is associative, then for all $a, t \in Q(A)$ the identity $a^{'} * t * a = t + a^{'}t + ta + a^{'}ta$ is valid.

(iii) If A is associative and unitary, then the restriction of the function $A \to A$, $a \mapsto 1_A + a$ to $Q(A)$ is a group isomorphism between $Q(A)$ and $E(A)$.$\diamond$

1.1.5 Proposition

For every associative K-algebra A the following statements are valid:

(i) For every subalgebra T of A the set $Q(T)$ is a subgroup of $Q(A)$.

(ii) For every ideal I of A the set $Q(I) = Q(A) \cap I$ is a normal subgroup of $Q(A)$.

Proof. ad(i): This statement is straightforward to prove.

ad(ii): Because of part (i) the set $Q(I)$ is a subgroup of $Q(A)$. For all $a \in Q(A) \cap I$ the identity $a^{'} = -a - aa^{'} \in I$ is valid, and hence $Q(A) \cap I = Q(I)$ is deduced. If $t \in Q(I)$ and $a \in Q(A)$ are valid, then we use part (ii) of remark 1.1.4 to conclude $a^{'} * t * a = t + a^{'}t + ta + a^{'}ta$. Thus, $a^{'} * t * a \in Q(A) \cap I = Q(I)$ is proven.$\diamond$

1.1.6 Definition (semidirect decomposition)

If A is a K-algebra, then we call a pair (I, T) a semidirect resp. direct decomposition of A, if A is the inner direct sum of the ideal I and the subalgebra resp. the ideal T of A.
For a group G a pair (N, U) is called a semidirect resp. direct decomposition of G, if G is the product of the normal subgroup N and of the subgroup resp. the normal subgroup U of G and $N \cap U = \{1_G\}$ is valid.$\diamond$

1.1.7 Proposition

If A is an associative K-algebra and (I, T) a semidirect decomposition of A, then $(Q(I), Q(T))$ is a semidirect decomposition of $Q(A)$.

Proof. By using proposition 1.1.5 the set $Q(I)$ is a normal subgroup and $Q(T)$ is a subgroup of $Q(A)$ such that their intersection is exactly $\{0_A\}$.

Let $q \in Q(A)$. Elements $i, j \in I$ and $t, s \in T$ exist such that $q = i + t$ and $q^{'} = j + s$ are valid. Because of $0_A = q * q^{'}$ and part (i) of remark 1.1.4 we deduce $0_A = t * s + i * j + tj + is$, and thus $t * s = 0_A$ is valid. The identity $0_A = q^{'} * q$ is used to prove $s * t = 0_A$ in a similar way. Hence, $t \in Q(T)$ and $t^{'} = s$ are true. We use part (i) of remark 1.1.4 to conduct $(i+is)*t = i*t+is+ist = i+t+it+is+ist = i+t+i\,(s*t) = q$. Because of $q \in Q(A)$ and $t \in Q(T)$ we deduce $i + is \in Q(A) \cap I$, and by using part (ii) of proposition 1.1.5 the proof is finished.$\diamond$

1.1.8 Corollary

Let (I, T) be a semidirect decomposition of an associative K-algebra A. The following statements are valid:

(i) If T is an ideal of A or T is central in A, then $(Q(I), Q(T))$ is a direct decomposition of $Q(A)$.

(ii) If A is unitary, then $(1_A + Q(I), 1_A + Q(T))$ is a semidirect decomposition of $E(A)$.

(iii) If A is unitary and $(Q(I), Q(T))$ is a direct decomposition of $Q(A)$, then $(1_A + Q(I), 1_A + Q(T))$ is a direct decomposition of $E(A)$.

Proof. ad(i): This statement is a direct consequence of proposition 1.1.7 and part (ii) of proposition 1.1.5 because $Q(T)$ is a normal subgroup of $Q(A)$ in the mentioned scenarios.

ad(ii) and (iii): These statements are a consequence of proposition 1.1.7 and part (iii) of proposition 1.1.5.$\diamond$

1.1.9 Definition

(i) If K is a field and $n \in \mathbb{N}_0$, then we define $n_K := \sum_{i=1}^{n} 1_K$.

(ii) For every finite subset M of a K-algebra A we define $\overline{M} := \sum_{m \in M} m$.
For a group G, a finite and non-empty subset H of G and a field K such that $char(K)$ is not dividing $\mid H \mid$ we define $e_H := \frac{1}{|H|_K}\overline{H}$.$\diamond$

1.1.10 Proposition (idempotents and subgroups)

Let G be a group, H a finite and non-empty subset of G and K a field such that $char(K)$ is not dividing $\mid H \mid$. e_H is an idempotent of KG if and only if H is a subgroup of G.

Proof. If H is a subgroup of G, then for all $h \in H$ the identity $h\overline{H} = \overline{H}$

is valid, and thus $\overline{H}^2 = \mid H \mid_K \overline{H}$ and $(e_H)^2 = e_H$ are valid.
If e_H is an idempotent of KG, then $\overline{H}^2 = \mid H \mid_K \overline{H}$ is true. Let $x, y \in H$. Elements $k \in K$ and $h \in H$ exist such that $kxy = \mid H \mid_K h$ is valid. If $xy \neq h$ would be true, then $\mid H \mid_K = 0_K$ would be valid which is a contradiction. Therefor $xy = h \in H$ is proven, and by using the finiteness of H we deduce that H is a subgroup of G.$\diamond$

1.1.11 Definition (isomorphism and span)

(i) If K is a field, then $\cong_K$, $\langle \dots \rangle_K$ etc. are called the isomorphism, the span etc. within the class of K-spaces.
By $\mathcal{A}$, $\mathcal{A}_1$, $\mathcal{L}$ resp. $\mathcal{G}$ we denote the class of associative algebras over K, the class of associative unitary algebras over K, the class of Lie algebras over K resp. the class of groups. If $\mathcal{X}$ is one of these classes, then we denote by $\cong_{\mathcal{X}}$, $\langle \dots \rangle_{\mathcal{X}}$ etc. the isomorphism, the span etc. within the class $\mathcal{X}$.

(ii) For all $n \in \mathbb{N}$ we define $\underline{n} := \mathbb{N}_{\leq n}$ and $\underline{n}_0 := \underline{n} \cup \{0\}$.$\diamond$

1.1.12 Definition (augmentation)

Let K be a field and V a finite-dimensional K-space. For every K-basis B of V we define $Aug_B(V) := \langle \{b_1 - b_2 \mid b_1, b_2 \in B\} \rangle_K$. If $v \in V$, then for every $b \in B$ exactly one $k_b \in K$ exists such that $v = \sum_{b \in B} k_b b$ is valid, and we define $aug_B(v) := \sum_{b \in B} k_b$. For a finite magma M we use the notation $Aug(KM) := Aug_M(KM)$ and call $Aug(KM)$ the augmentation ideal of KM. If $x \in KM$, then $aug(x) := aug_M(x)$ is defined and called the augmentation of x.$\diamond$

1.1.13 Remark (augmentation ideal)

Let K be a field, M a finite non-empty magma and $aug : KM \to K$ the K-linear extension of the function $M \longrightarrow K$, $m \mapsto 1_K$. The augmentation function aug is an algebra-epimorphism such that $ker(aug) = Aug(KM)$ is valid. In particular, $Aug(KM)$ is an ideal of codimension 1 (and hence a maximal ideal) of KM. For every $m \in M$ the set $\{x - m \mid x \in M \setminus \{m\}\}$ is a K-basis of $Aug(KM)$.$\diamond$

1.1.14 Definition and remark (kernel of the augmentation map)

Let K be a field, G a finite group, N a normal subgroup of G and $p_N : KG \longrightarrow K(G/N)$ the linearization of the $\mathcal{G}$-epimorphism $G \longrightarrow G/N$, $g \mapsto Ng$. By using lemma 1.8 of chapter 1 in [51] the kernel of p_N is exactly $KG\, Aug(KN) = Aug(KN)\, KG$.$\diamond$

For the following lemma several proofs are existing (see e.g. D.A.R. Wallace in [74], L.E. Dickson[1] in [23] or R.L. Kruse and D.T. Price in [37]). We

[1]Leonard Eugene Dickson (January 22, 1874 to January 17, 1954) was an American mathematician. He was one of the first American researchers in abstract algebra, in particular the theory of finite fields and classical groups, and is also remembered for a three-volume history of number theory, History of the Theory of Numbers.

Dickson considered himself a Texan by virtue of having grown up in Cleburne, where his father was a banker, merchant, and real estate investor. He attended the University of Texas at Austin, where George Bruce Halsted encouraged his study of mathematics. Dickson earned a B.S. in 1893 and an M.S. in 1894, under Halsted's supervision. Dickson first specialised in Halsted's own specialty, geometry.

Both the University of Chicago and Harvard University welcomed Dickson as a Ph.D. student, and Dickson initially accepted Harvard offer, but chose to attend Chicago instead. In 1896, when he was only 22 years of age, he was awarded Chicago's first doctorate in mathematics, for a dissertation titled The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group, supervised by E. H. Moore.

Dickson then went to Leipzig and Paris to study under Sophus Lie and Camille Jordan, respectively. On returning to the USA, he became an instructor at the University of California. In 1899 and at the extraordinarily young age of 25, Dickson was appointed associate professor at the University of Texas. Chicago countered by offering him a position in 1900, and he spent the balance of his career there. At Chicago, he supervised 53 Ph.D. theses; his most accomplished student was probably A. A. Albert. He was a visiting professor at the University of California in 1914, 1918, and 1922. In 1939, he returned to Texas to retire.

Dickson married Susan McLeod Davis in 1902; they had two children, Campbell and Eleanor.

Dickson was elected to the National Academy of Sciences in 1913, and was also a member of the American Philosophical Society, the American Academy of Arts and Sciences, the London Mathematical Society, the French Academy of Sciences and the Union of Czech Mathematicians and Physicists. Dickson was the first recipient of a prize created in 1924 by The American Association for the Advancement of Science, for his work on the arithmetics of algebras. Harvard (1936) and Princeton (1941) awarded him honorary doctorates.

Dickson presided over the American Mathematical Society in 1917 to 1918. His December 1918 presidential address, titled 'Mathematics in War Perspective,' criticized American mathematics for falling short of those of Britain, France, and Germany: 'Let it not again become possible that thousands of young men shall be so seriously handicapped in their Army and Navy work by lack of adequate preparation in mathematics.' In 1928, he was also the first recipient of the Cole Prize for algebra, awarded annually by the AMS, for his book Algebren und ihre Zahlentheorie.

It appears that Dickson was a hard man: 'A hard-bitten character, Dickson tended to speak his mind bluntly; he was always sparing in his praise for the work of others. ... he indulged his serious passions for bridge and billiards and reportedly did not like to lose at either game. He delivered terse and unpolished lectures and spoke sternly to his students. ... Given Dickson's intolerance for student weaknesses in mathematics, however, his comments could be harsh, even though not intended to be personal. He did not aim to make students feel good about themselves. Dickson had a sudden death trial for his prospective doctoral students: he assigned a preliminary problem which was shorter than a dissertation problem, and if the student could solve it in three months, Dickson would agree to oversee the graduate student's work. If not the student had to look elsewhere for an advisor.'

Dickson had a major impact on American mathematics, especially abstract algebra. His mathematical output consists of 18 books and more than 250 papers. The Collected present another approach.

Mathematical Papers of Leonard Eugene Dickson fill six large volumes.

In 1901, Dickson published his first book Linear groups with an exposition of the Galois field theory, a revision and expansion of his Ph.D. thesis. Teubner in Leipzig published the book, as there was no well-established American scientific publisher at the time. Dickson had already published 43 research papers in the preceding five years; all but seven on finite linear groups. Parshall (1991) described the book as follows: 'Dickson presented a unified, complete, and general theory of the classical linear groups – not merely over the prime field $GF(p)$ as Jordan had done – but over the general finite field $GF(p^n)$, and he did this against the backdrop of a well-developed theory of these underlying fields. His book represented the first systematic treatment of finite fields in the mathematical literature.' An appendix in this book lists the non-Abelian simple groups then known having order less than 1 billion. He listed 53 of the 56 having order less than 1 million. The remaining three were found in 1960, 1965, and 1967. Dickson worked on finite fields and extended the theory of linear associative algebras initiated by Joseph Wedderburn and Cartan. He started the study of modular invariants of a group. In 1905, Wedderburn, then at Chicago on a Carnegie Fellowship, published a paper that included three claimed proofs of a theorem stating that all finite division algebras were commutative, now known as Wedderburn's theorem. The proofs all made clever use of the interplay between the additive group of a finite division algebra A, and the multiplicative group. Karen Parshall noted that the first of these three proofs had a gap not noticed at the time. Dickson also found a proof of this result but, believing Wedderburn's first proof to be correct, Dickson acknowledged Wedderburn's priority. But Dickson also noted that Wedderburn constructed his second and third proofs only after having seen Dickson's proof. She concluded that Dickson should be credited with the first correct proof.

Dickson's search for a counterexample to Wedderburn's theorem led him to investigate non-associative algebras, and in a series of papers he found all possible three and four-dimensional (non-associative) division algebras over a field.

In 1919 Dickson constructed Cayley numbers by a doubling process starting with quaternions. His method was extended to a doubling of the real numbers to produce the complex numbers, and of the complex numbers to produce the real quaternions by A. A. Albert in 1922, and the procedure is known now as the Cayley-Dickson construction of composition algebras.

Dickson proved many interesting results in number theory, using results of Vinogradov to deduce the ideal Waring theorem in his investigations of additive number theory. He proved the Waring's problem for $k = 7$ $k \geq 7k \geq 7$ under the further condition of $(3k+1)/(2k-1) = [1.5k] + 1(3^k+1)/(2^k-1) \leq [1.5^k] + 1(3^k+1)/(2^k-1) \leq [1.5^k] + 1$ independently of Subbayya Sivasankaranarayana Pillai who proved it for $k = 6$ $k \geq 6k \geq 6$ ahead of him.

The three-volume History of the Theory of Numbers (1919 to 1923) is still much consulted today, covering divisibility and primality, Diophantine analysis, and quadratic and higher forms. The work contains little interpretation and makes no attempt to contextualize the results being described, yet it contains essentially every significant number theoretic idea from the dawn of mathematics up to the 1920s except for quadratic reciprocity and higher reciprocity laws. A planned fourth volume on these topics was never written. A. A. Albert remarked that this three volume work 'would be a life's work by itself for a more ordinary man.'