University of Trento
Faculty of Mathematical, Physical and Natural Sciences

Unit group for abelian group algebras

Paolo Faccin and Willem A. de Graaf

May 31, 2011

Outline

Outline

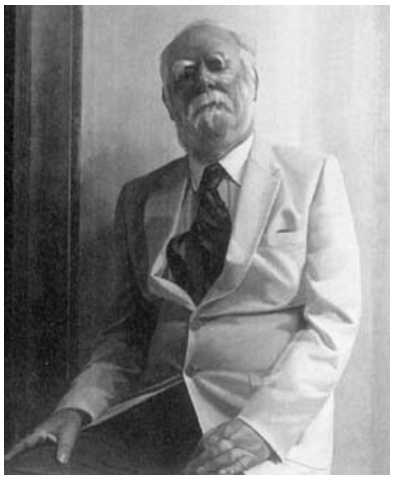
Definition

Let G be an abelian group of order n, and consider the set:

$$\mathbb{Q}G := \{\sum_{g \in G} a_g g \quad | \quad a_g \in \mathbb{Q}\}$$

this is called the **Group algebra over** $\mathbb{Q}$.
We define its unit group as the set:

$$(\mathbb{Z}G)^* := \{u \in \mathbb{Z}G \quad | \quad u^{-1} \in \mathbb{Z}G\}$$

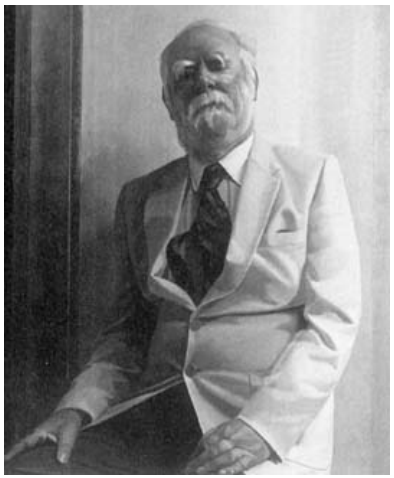


In 1940 on his doctoral thesis Graham Higman proved that:

$$(\mathbb{Z}G)^* = \pm G \times F$$

where F is a free abelian group of finite rank.

Problem: How find generators of $(\mathbb{Z}G)^*$?



In 1940 on his doctoral thesis Graham Higman proved that:

$$(\mathbb{Z}G)^* = \pm G \times F$$

where F is a free abelian group of finite rank.

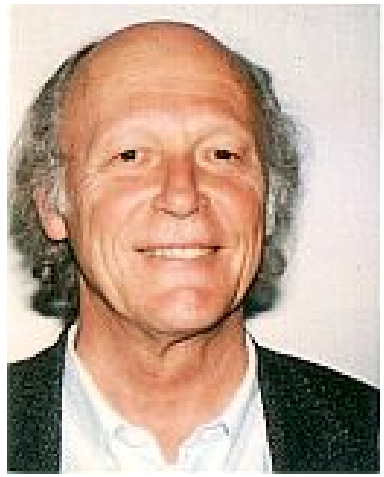
Problem: How find generators of $(\mathbb{Z}G)^*$?

In 1966 Hyman Bass constructed a subgroup of $(\mathbb{Z}G)^*$ of finite index, using his cyclic units $\mathcal{B}$.

In 1992 Klaus Hoechsmann gave generators of a subgroup $\mathcal{H}$ of $(\mathbb{Z}G)^*$ of smaller index.
He called them **constructible units**.

In 1966 Hyman Bass constructed a subgroup of $(\mathbb{Z}G)^*$ of finite index, using his cyclic units $\mathcal{B}$.

In 1992 Klaus Hoechsmann gave generators of a subgroup $\mathcal{H}$ of $(\mathbb{Z}G)^*$ of smaller index.
He called them **constructible units**.



Group G	**Index** $[\mathcal{H} : \mathcal{B}]$
C_{10}	4
C_{17}	33554432
C_{18}	144
C_{19}	1224440064
C_{24}	512
C_{27}	14693280768
$C_3 \times C_9$	1728
C_{30}	65536
C_{31}	318864600000000000

"Does this method ever yield all units, if $n = |G|$ is not a prime power? That answer seems to be affermative for $n < 74$."

Hoechsmann

We have developed an algorithm for computing generators of $(\mathbb{Z}G)^*$. It is implemented in *Magma*.

With this we have calculated all generators when $|G| \leq 50$,
With three exceptions:

$$C_2 \times C_2 \times C_2 \times C_6, \qquad C_7 \times C_7, \qquad C_5 \times C_{10}$$

And for some groups of order ≤ 60

We obtain *exotic* units for some groups:

- C_{40}
- $C_2 \times C_{20}$
- $C_2 \times C_2 \times C_{10}$
- $C_2 \times C_{30}$
- C_{48}
- $C_2 \times C_{24}$
- $C_4 \times C_{12}$
- C_{60}

In all cases $[(\mathbb{Z}G)^* : \mathcal{H}] = 2$, except for $C_4 \times C_{12}$, where it is 4.

Outline

Notation

Let:

- G be an abelian group of order n,
- $\mathbb{Q}(\omega_n)$ be the n-th cyclotomic field,
- $\mathcal{U}$ be the unit group of $\bigoplus_{d|n} a_d\mathbb{Z}(\omega_d)$,
- $\mathcal{H}$ be the group of *Hoechsmann*'s units.

Theorem

There exists an isomorphism:

$$\phi : \mathbb{Q}G \longrightarrow \bigoplus_{d|n} a_d \mathbb{Q}(\omega_d),$$

It also holds that $(\mathbb{Z}G)^*$ **has finite index** *in* $\phi^{-1}(\mathcal{U})$

$$\mathcal{H} \trianglelefteq (\mathbb{Z}G)^* \trianglelefteq \phi^{-1}(\mathcal{U})$$

$$\mathcal{H} \trianglelefteq (\mathbb{Z}G)^* \trianglelefteq \phi^{-1}(\mathcal{U})$$

$$\mathcal{H} \trianglelefteq (\mathbb{Z}G)^*$$

This index is finite, but unknown

$$\mathcal{H} \trianglelefteq (\mathbb{Z}G)^* \trianglelefteq \phi^{-1}(\mathcal{U})$$

$$(\mathbb{Z}G)^* \trianglelefteq \phi^{-1}(\mathcal{U})$$

This index is finite, but unknown

Also this index is finite, but unknown

$$\mathcal{H} \trianglelefteq (\mathbb{Z}G)^* \trianglelefteq \phi^{-1}(\mathcal{U})$$

$$\mathcal{H} \trianglelefteq \phi^{-1}(\mathcal{U})$$

This index is finite, but unknown

Also this index is finite, but unknown

Instead, this index is finite, and computable

Idea of the algorithm

For all primes p dividing the index $[\phi^{-1}(\mathcal{U}) : \mathcal{H}]$, construct:

- $\mathcal{H}^p$,
- $\phi^{-1}(\mathcal{U})^p$
- $M_p = (\phi^{-1}(\mathcal{U})^p \cap \mathcal{H})/\mathcal{H}^p$, and
- $\mathcal{U}_p = \{u \in \phi^{-1}(\mathcal{U}) \mid u^p = 1\}$.

- For all $m \in M_p$, $m \neq 1$, get $u \in \phi^{-1}(\mathcal{U})$ such that the coset $u^p\mathcal{H}^p$ is equal to m.
- For each $v \in \mathcal{U}_p$ check if both uv and $(uv)^{-1}$ lie in $\mathbb{Z}G$.
- If so,then add uv to $\mathcal{H}$.

Outline

Construction of the isomorphism

Our method is based on the existence of an isomorphism:

$$\phi : \mathbb{Q}G \longrightarrow \bigoplus_{d|n} a_d \mathbb{Q}(\omega_d),$$

where a_d is the number of cyclic subgroups of G of order d. We can compute it using well-known algorithms for associative algebras.

Units in cyclotomic fields $\mathbb{Q}(\omega_n)$

n is a power of prime

It is known how to construct a subgroup U_n of the unit group, such that its index in the full group of units is h_n^+.

- if $\varphi(n) < 66$, or
- if $\varphi(n) < 162$ and we assume the Generalised Riemann Hypothesis

then, $h_n^+ = 1$.

n is not a power of prime

On 1996 Cornelius Greither presented a method to construct a subgroup U_n of the unit group, whose index depend on h_n^+,such that:

- if $n < 130$ and $\varphi(n) \leq 72$ or
- if $n < 130$ and we assume the Generalised Riemann Hypothesis

its index in the full group of units is **finite** and **easily computable**, as $h_n^+ = 1$ in those cases.

Recently, Claus Fieker has written in *Magma* V2.17-2 a program that, given:

- a number field $\mathbb{Q}(\omega_n)$,
- a finite-index subgroup U_n of the unit group $\mathbb{Z}(\omega_n)^*$
- and a prime p dividing the index of U_n in $\mathbb{Z}(\omega_n)^*$

Computes a subgroup $\bar{U}_n$ of $\mathbb{Z}(\omega_n)^*$ such that:

- $U_n \subset \bar{U}_n$
- and p does not divide the index $[\mathbb{Z}(\omega_n)^* : \bar{U}_n]$.

Multiplicative relations and index

We let $b_1, \cdots, b_r$ be units in $\mathbb{Q}G$ and let B be the group generated by them. Computing its normal generating set is equivalent to find a basis of the lattice:

$$\Lambda := \{(e_1, \cdots, e_r) \in \mathbb{Z}^r \mid b_1^{e_1} \cdots b_r^{e_r} = 1\}$$

Ge's algorithm can be used to solve this problem. Also, using this algorithm we can compute the index of a subgroup C of B.

Exotic units

$C_4 \times C_{12} = \langle x, y \mid x^4 = y^{12} = 1 \rangle$; index is 4;
quotient group is $C_2 \times C_2$:

$$-8 + 4y + 4y^2 - 4y^3 + 8y^4 - 4y^5 + 7y^6 - 7y^7 - 7y^{10} + 7y^{11} - 9x + 4xy + 4xy^2 - 4xy^3 + 8xy^4 - 4xy^5 + 7xy^6 - 7xy^7 - 7xy^{10} + 7xy^{11} - 8x^2 + 4x^2y + 4x^2y^2 - 4x^2y^3 + 8x^2y^4 - 4x^2y^5 + 7x^2y^6 - 7x^2y^7 - 7x^2y^{10} + 7x^2y^{11} - 8x^3 + 4x^3y + 4x^3y^2 - 4x^3y^3 + 8x^3y^4 - 4x^3y^5 + 7x^3y^6 - 7x^3y^7 - 7x^3y^{10} + 7x^3y^{11}$$

$$-8 + 4y + 4y^2 - 4y^3 + 8y^4 - 4y^5 + 7y^6 - 7y^7 - 7y^{10} + 7y^{11} + 8x - 4xy - 4xy^2 + 4xy^3 - 9xy^4 + 4xy^5 - 7xy^6 + 7xy^7 + 7xy^{10} - 7xy^{11} - 7x^2y + 7x^2y^2 - 7x^2y^3 + 7x^2y^5 + 4x^2y^6 + 4x^2y^7 - 8x^2y^8 + 8x^2y^9 - 4x^2y^{10} - 4x^2y^{11} + 7x^3y - 7x^3y^2 + 7x^3y^3 - 7x^3y^5 - 4x^3y^6 - 4x^3y^7 + 8x^3y^8 - 8x^3y^9 + 4x^3y^{10} + 4x^3y^{11}$$

$C_{60} = \langle x \mid x^{60} = 1 \rangle$; index is 2

$$1070470425 - 1111305318x + 589543337x^2 + 228051317x^3 - 922900338x^4 + 1139421655x^5 - 767669910x^6 - x^7 + 767669909x^8 - 1139421656x^9 + 922900338x^{10} - 228051317x^{11} - 589543337x^{12} + 1111305318x^{13} - 1070470426x^{14} + 489040910x^{15} + 333357000x^{16} - 973259882x^{17} + 1101026911x^{18} - 650380744x^{19} - 147570087x^{20} + 883254000x^{21} - 1179086675x^{22} + 883254000x^{23} - 147570087x^{24} - 650380744x^{25} + 1101026911x^{26} - 973259882x^{27} + 333357000x^{28} + 489040910x^{29} - 1070470426x^{30} + 1111305318x^{31} - 589543337x^{32} - 228051317x^{33} + 922900338x^{34} - 1139421656x^{35} + 767669909x^{36} - x^{37} - 767669910x^{38} + 1139421655x^{39} - 922900338x^{40} + 228051317x^{41} + 589543337x^{42} - 1111305318x^{43} + 1070470425x^{44} - 489040910x^{45} - 333357000x^{46} + 973259883x^{47} - 1101026910x^{48} + 650380745x^{49} + 147570088x^{50} - 883254000x^{51} + 1179086676x^{52} - 883254000x^{53} + 147570088x^{54} + 650380745x^{55} - 1101026910x^{56} + 973259883x^{57} - 333357000x^{58} - 489040910x^{59}$$

Practical experiences

The main bottlenecks of the algorithm are due to:

- the size of the set $M_p \times U_p$. If it gets too large, it becomes impossible to run through the set.
- the multplicative relations between elements.

This is why we failed when G is $C_2 \times C_2 \times C_2 \times C_6$, $C_7 \times C_7$ and $C_5 \times C_{10}$.

group	max $\lvert M_p\rvert \cdot \lvert U_p\rvert$	multrel. time (s)	tot. time (s)
C_{38}	73	494	509
C_{39}	28561	726	796
C_{40}	32768	871	985
$C_2 \times C_{20}$	524288	170	344
$C_2 \times C_2 \times C_{10}$	1048576	77	602
C_{43}	7	2501	2697
C_{48}	524288	1132	2414
$C_2 \times C_{24}$	67108864	195	32119

Table: Running times of the algorithm with as input some groups of around 40 elements. The timings were done on a 3.16 GHz processor.

Bibliography

- http://www.science.unitn.it/~degraaf/units.html
- G. Ge. Algorithms related to multiplicative representations of algebraic numbers. PhD thesis, University of California, Berkeley, 1993
- Cornelius Greither. Improving Ramachandra's and Levesque's unit index. In Number theory (Ottawa, ON, 1996), volume 19 of CRM Proc. Lecture Notes, pages 111–120. Amer. Math. Soc., Providence, RI, 1999.
- Klaus Hoechsmann. Constructing units in commutative group rings. Manuscripta Math., 75(1):5–23, 1992.

Thank you