On Fuchs' problem on the group of units of a ring: the state of the art and some progress using braces

Ilaria Del Corso

Omaha, May 30, 2022

Dipartimento di Matematica
Università di Pisa

Fuchs’ question

Fuchs' questions

In Fuchs' book "Abelian Groups" (1960) the following question is posed (Problem 72)

> Characterize the groups which are the (abelian) groups of all units in a commutative and associative ring with identity.

The general problem appeared to be very difficult and it is still open. Partial approaches

- to restrict the class of rings
- to restrict the class of groups
- to restrict both
- Ditor's question (1971). Which whole numbers can be the number of units of a ring?

The history of the problem

Units of number rings

Theorem (Dirichlet (1846))

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. Let $[K : \mathbb{Q}] = r + 2s$ (here r is the number of real embeddings of K in $\bar{\mathbb{Q}}$ and $2s$ the number of non-real embeddings). Then

$$\mathcal{O}_K^* \cong T \times \mathbb{Z}^{r+s-1}$$

where T is the (cyclic) group of the roots of unity contained in K.

Units in group rings

Let R be a ring and let G be a group. The group ring RG is defined by

$$RG = \{\sum_{g \in G} \lambda_g g \mid \lambda_g \in R \text{ and } \lambda_g = 0 \text{ for almost all } g\}.$$

Theorem (Higman 1940) Let G be a finite abelian group of order n. Then

$$(\mathbb{Z}G)^* \cong \pm G \times \mathbb{Z}^{r_G}$$

where $r_G = \frac{1}{2}(n + 1 + c_2 - 2l)$, with
$c_d = \#\{\text{cyclic subgroups of order d of } G\}$ and $l = \sum_{d|n} c_n$.

More recently

- Pearson and Schneider (1970): Classification of the realizable cyclic groups.
- Chebolu and Lockridge (2015): Classification of the realizable indecomposable abelian groups.
- idc, Dvornicich (BLMS 2018 AMPA 2018)
  • Classification of the finite abelian groups realizable in the class of the integral domains/torsion-free rings/reduced rings.
  • For general rings $\rightarrow$ Necessary conditions for a finite ab. group to be realizable.
  $\rightarrow$ Infinite new families of realizable/non-real. finite abelian groups.
- idc (JLMS 2020) Classification of the finitely generated abelian groups which can be realized in the class of the integral domains, of the torsion-free rings and of the reduced rings.
- idc (work in progress) Some progress on classification using braces (radical rings).

Finitely generated abelian groups

Finitely generated abelian groups

Fuchs' question for finitely generated abelian groups

A ring with 1, A^* group of units of A. Assume that A^* is finitely generated and abelian

$$A^* \cong (A^*)_{tors} \times \mathbb{Z}^{r_A}$$

Problem: what groups arise?

- T finite abelian group: $\exists\ A \in \mathcal{C}$ such that $(A^*)_{tors} \cong T$?

- If $(A^*)_{tors} \cong T$ what can we say on $r_A = \mathrm{rank}(A^*)$?

Reduction step 1

Let $A_0 (= \mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z})$ be the fundamental subring of A and consider the ring $R = A_0[(A^*)_{tors}]$.

Clearly $R^* \leq A^*$, therefore

$$r_A \geq r_R$$

and also

$$(A^*)_{tors} = (R^*)_{tors}.$$

So, up to changing $A \longleftrightarrow R = A_0[(A^*)_{tors}]$, we can restrict to study:

commutative rings which are finitely generated and integral over A_0.

Results for special classes of rings

Integral domains

Theorem (idc JLMS 2020)

The finitely generated abelian groups that occur as groups of units of an integral domain are:

i) $\mathrm{char}(A) = p$*: all groups of the form* $\mathbb{F}_{p^n}^* \times \mathbb{Z}^r$ *with* $n \geq 1$ *and* $r \geq 0$*;*
ii) $\mathrm{char}(A) = 0$*: all groups of the form* $\mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}^r$*, with* $n \geq 1$*,*
$r \geq \frac{\phi(2n)}{2} - 1$*.*

Corollary

The finite abelian groups that occur as groups of units of an integral domain A are:

i) the multiplicative groups of the finite fields if $\mathrm{char}(A) > 0$*;*

ii) the cyclic groups of order 2,4, or 6 if $\mathrm{char}(A) = 0$*.*

Torsion-free rings

A is *torsion-free* if 0 is the only element of finite additive order. In this case, $\mathrm{char}(A) = 0$.
Example: If R is a torsion-free ring and G is a group, then RG is torsion-free.

Theorem (idc JLMS 2020)

Let T be a finite abelian group of even order. Then there exists an explicit constant $g(T)$ such that the following holds:

$$T \times \mathbb{Z}^r$$

is the group of units of a torsion-free ring if and only if $r \geq g(T)$.

$$T \cong \prod_{\iota=1}^{s} \mathbb{Z}/p_\iota^{a_\iota}\mathbb{Z} \times \prod_{i=1}^{\rho} \mathbb{Z}/2^{\epsilon_i}\mathbb{Z} \times (\mathbb{Z}/2^{\epsilon}\mathbb{Z})^{\sigma}$$

where $s, \rho \geq 0$, $\sigma \geq 1$ and

- for all $\iota = 1, \ldots, s$ the p_ι's are odd prime numbers, not necessarily distinct, and $a_\iota \geq 1$;

- $\epsilon = \epsilon(T) \geq 1$ and $\epsilon_i > \epsilon$ for all $i = 1, \ldots, \rho$.

$$g(T) = \sum_{\iota=1}^{s}\left(\frac{\phi(2^{\epsilon} p_\iota^{a_\iota})}{2} - 1\right) + \sum_{i=1}^{\rho}\left(\frac{\phi(2^{\epsilon_i})}{2} - 1\right) + c(T)$$

where

$$c(T) = \begin{cases} (\sigma - s)\left(\frac{\phi(2^{\epsilon})}{2} - 1\right) & \text{for } s < \sigma \text{ and } \epsilon > 1 \\ 0 & \text{for } s_0 \leq \sigma \leq s \text{ or } \epsilon = 1 \\ \left\lceil \frac{\phi(2^{\epsilon})}{2} - 1 \right\rceil & \text{for } \sigma < s_0 \end{cases}$$

where $s_0 = \#\{p_1, \ldots, p_s\}$.

Corollary (idc, R.Dvornicich BLMS 2018)

The finite abelian groups which are the group of units of a torsion-free ring A, are all those of the form

$$(\mathbb{Z}/2\mathbb{Z})^a \times (\mathbb{Z}/4\mathbb{Z})^b \times (\mathbb{Z}/3\mathbb{Z})^c$$

where $a, b, c \in \mathbb{N}$, $a + b \geq 1$ *and* $a \geq 1$ *if* $c \geq 1$.

In particular, the possible values of $|A^*|$ *are the integers* $2^d 3^c$ *with* $d \geq 1$.

Reduced rings

Theorem (idc JLMS 2020)

The finitely generated abelian groups that occur as groups of units of a reduced ring are those of the form

$$\prod_{i=1}^{k} \mathbb{F}^*_{p_i^{n_i}} \times T \times \mathbb{Z}^g$$

where $k, n_1, \ldots, n_k$ are positive integers, $\{p_1, \ldots, p_k\}$ are, not necessarily distinct, primes, T is any finite abelian group of even order and $g \geq g(T)$.

Tools

An exact sequence

Let $\mathfrak{N} = \{a \in A \mid a^n = 0 \text{ for some } n \in \mathbb{N}\}$ be the nilradical of A. Clearly $1 + \mathfrak{N} < A^*$, so we have the following exact sequence:

$$1 \to 1 + \mathfrak{N} \to A^* \to A^*/(1 + \mathfrak{N}) \to 1$$

$$1 \to 1 + \mathfrak{N} \to A^* \to (A/\mathfrak{N})^* \to 1$$

The quotient ring $A/\mathfrak{N}$ is *reduced*, namely, its nilradical is trivial.

This exact sequence does not split in general.

Reduction step 2: splitting of the ring

Proposition (Pearson & Schneider 1970)

Let A be a commutative ring which is finitely generated and integral over its fundamental subring. Then $A = A_1 \oplus A_2$, where A_1 is a finite ring and the torsion ideal of A_2 is contained in its nilradical.

We will say that A is *of type 2* if its torsion ideal is contained in the nilradical.

If A is a type 2 ring $\Rightarrow \mathrm{char}(A) = 0$ since 1 is not nilpotent.

We can split the problem in the study of the units of finite rings and of characteristic 0 rings of type 2.

Finite rings

Finite rings

Let A be finite and commutative, then A is artinian and therefore $A \cong A_1 \times \cdots \times A_s$ (where A_i are *local* artinian rings) and

$$A^* \cong A_1^* \times \cdots \times A_s^*.$$

Let $(A, \mathfrak{m})$ be finite a local ring, and let $\mathrm{char}(A) = p^c$. In this case $\mathfrak{N} = \mathfrak{m}$ and the exact sequence is

$$1 \to 1 + \mathfrak{N} \hookrightarrow A^* \to (A/\mathfrak{N})^* \to 1$$

$$1 \to 1 + \mathfrak{m} \hookrightarrow A^* \to \mathbb{F}_{p^\lambda}^* \to 1$$

This sequence is split and therefore

$$A^* \cong (A/\mathfrak{m})^* \times (1 + \mathfrak{m}) \cong \mathbb{F}_{p^\lambda}^* \times (1 + \mathfrak{m}).$$

What can we say on the abelian p-group $1 + \mathfrak{m}$?

The abelian p-group $1 + \mathfrak{m}$.

- $|1 + \mathfrak{m}| = p^{k\lambda}$ for some $k \geq 0$
- Positive results. $\forall\, P$ abelian p-group there exists $(A, \mathfrak{m})$ with

$$A^* \cong \mathbb{F}_{p^\lambda}^* \times P^\lambda.$$

  In particular, all groups of type $\mathbb{F}_p^* \times P$ are the groups units of finite local rings. Here $p > 2$.

- On the negative side $\rightarrow 1 + \mathfrak{m}$ can be different from P^λ, but it can not be any p-group if $\lambda > 1$ and not even any group of cardinality $p^{k\lambda}$.

  Example: For $\lambda > 1$, the group $1 + \mathfrak{m}$ can not be cyclic.

  The presence of a "big" residue field gives an obstruction.

Characteristic zero rings

Characteristic 0 rings

We now restrict to the case when A^* is a **finite abelian** group.

Theorem (idc, R.Dvornicich)

If $\mathrm{char}(A) = 0$, *then*

$$A^* \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times H \\ \mathbb{Z}/4\mathbb{Z} \times H \end{cases},$$

where H *is finite and abelian.*

As a partial converse, we have that every group of type

$$\mathbb{Z}/2\mathbb{Z} \times H,$$

where H *is a finite abelian group, occur as group of units of a characteristic 0 ring.*

The last theorem, together with the result on finite rings, allows us to completely answer Ditor's question for rings of any characteristic.

Corollary

- The possible values of $|A^*|$, when A is a characteristic 0 ring with finite group of units, are all the even positive integers.
- The possible values of $|A^*|$, when A is a ring with finite group of units, are all the even positive integers and the finite products of integers of the form $2^\lambda - 1$ with $\lambda \geq 1$.

The case $\epsilon = 2$

We have seen that

$$A^* \cong \mathbb{Z}/2^\epsilon\mathbb{Z} \times H \text{ with } \epsilon = 1 \text{ or } 2$$

For $\epsilon = 1$ all groups H are possible.

The same is no longer true for rings with $\epsilon = 2$.

Example: We can not have $H \cong \mathbb{Z}/11\mathbb{Z}$, since the cyclic group $\mathbb{Z}/44\mathbb{Z}$ is not realizable.

$$\text{If } \epsilon(A) = 2, \text{ then } \mathbb{Z}[i] \subseteq A.$$

The presence of the ring $\mathbb{Z}[i]$ is the obstruction in this case.

Consider the exact sequence

$$1 \to 1 + \mathfrak{N} \to A^* \to (A/\mathfrak{N})^* \to 1$$

and the exact sequence induced on the p-Sylow

$$1 \to (1 + \mathfrak{N})_p \to (A^*)_p \to (A/\mathfrak{N})_p^* \to 1.$$

This can be rewritten as

$$1 \to (1 + \mathfrak{N}_p) \to (A^*)_p \to B_p^* \to 1$$

where $B = A/\mathfrak{N}$.

If **A** is a **type 2 ring**, then the ring B is torsion-free and B^* is described by our classification. In particular,

$(B^*)_p$ is trivial for $p > 3$ and also for $p = 3$ if $\epsilon(A) = 2$.

Hence

$$(A^*)_p = 1 + \mathfrak{N}_p \ \forall p \geq 3.$$

In the case when A is of type 2 with $\epsilon(A) = 2$ we have found some necessary and some sufficient conditions, which are indeed very strict but not conclusive.

- $p \equiv 1 \pmod 4$: $(A^*)_p = 1 + \mathfrak{N}_p$ can be any abelian p-group.
- $p \equiv 3 \pmod 4$:
  - $(A^*)_p = 1 + \mathfrak{N}_p$
  - it can not be any p-group (e.g. it can not be cyclic),
  - the cardinality of $(A^*)_p$ must be a square,
  - and all squares of a p-group are realizable.
- $p = 2$: we have an exact sequence

$$1 \to 1 + \mathfrak{N}_2 \to (A^*)_2 \to (\mathbb{Z}/2\mathbb{Z})^a \times (\mathbb{Z}/4\mathbb{Z})^b \to 1$$

  where $a + b \geq 1$. We have a (not exhaustive) list of realizable 2-Sylow subgroups of A^*.

The radical ring $\mathfrak{N}$

The radical ring $\mathfrak{N}$

Both in the case $char(A) > 0$ and in the case $char(A) = 0$, we are left to study the group

$$1 + \mathfrak{N}$$

• When $char(A) > 0$ and A local $\implies A^* \cong \mathbb{F}^*_{p^\lambda} \times 1 + \mathfrak{N}$
the knowledge of $1 + \mathfrak{N}$ would be enough the conclude the characterization of the groups of units arising in this case.

• When $char(A) = 0 \implies A^*_p = 1 + \mathfrak{N}_p$, for $p > 2$
(the knowledge of $1 + \mathfrak{N}_2$ is not sufficient to determine the 2-Sylow of A^*.)

$\mathfrak{N}$ is a radical ring, so we can consider on it the adjoint operation $\circ$ defined by

$$x \circ y = x + y + xy, \qquad \forall x, y \in \mathfrak{N}$$

we have that $(\mathfrak{N}, +, \circ)$ is a (two-sided) brace and $1 + \mathfrak{N} \cong (\mathfrak{N}, \circ)$.

The following theorem gives some relation between the two group structures of a brace.
(For a p-group G we call $\mathrm{rank}(G)$ is the maximum r such that G has a subgroup of exponent p and order p^r. If G is abelian it is the number of cyclic factors of its decomposition as a product of cyclic groups)

Theorem (FCC12 - Bac16 - Caranti idc 22)

Let p be a prime, and let $(G, +, \circ)$ be a brace of order a power of the prime p. Then

$$rank(G, +) < p - 1 \iff rank(G, \circ) < p - 1.$$

When these conditions hold, $(G, +)$ and $(G, \circ)$ have the same rank, and each element has the same order in $(G, +)$ and $(G, \circ)$.

[FCC12] $\Longrightarrow$ if $\mathrm{rank}(\mathfrak{N}_p) < p-1$ then $1+\mathfrak{N}_p \cong \mathfrak{N}_p$

Q1 What kind of abelian group can be $\mathfrak{N}_p$?

Q2 Can we weaken the condition on the rank in [FCC12] and get the same result for $1+\mathfrak{N}_p$?

Q1: we are looking for some *general* information on $\mathfrak{N}p$.

Q2 seems to be hopeless: [FCC12] has been refined by Bachiller and by Caranti and myself, but well known examples show that it can not be generalized to braces (or radical rings) of rank$= p-1$, so we have to understand what kind of generalization is possible.

Q1

Consider the case $(A, \mathfrak{m})$ local with $A/\mathfrak{m} \cong \mathbb{F}^*_{p^\lambda}$, but everything has an analog for characteristic 0 rings!

In this case $\mathfrak{N} = \mathfrak{N}_p = \mathfrak{m}$.

$\mathfrak{m}$ can be the λ power of any abelian p-group.

In fact, let $P \cong \mathbb{Z}/p^{a_0}\mathbb{Z} \times \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$ $(a_0 \geq a_i)$.

Define $R = \frac{(\mathbb{Z}/p^{a_0+1}\mathbb{Z})[t]}{(f(t))}$ where $f(t)$ is irreducible modulo p of degree λ. Then

$$A = \frac{R[x_1, \dots x_r]}{(p^{a_i}x_i, x_i x_j)_{1 \leq i,j \leq r}}$$

is such that $\mathfrak{m} \cong P^\lambda$.

Q1

The following Theorem shows that also the converse holds, i.e.

$\mathfrak{m}$ is always the λ power of an abelian p-group.

Theorem

$(A, \mathfrak{m})$ local, with $A/\mathfrak{m} \cong \mathbb{F}_{p^\lambda}$. Then,

$$\mathfrak{m} \cong P^\lambda$$

where P is an abelian p-group.

Sketch of the proof. Let $D_\lambda = \mathbb{Z}_p[\zeta_{p^\lambda - 1}]$, where $\zeta_{p^\lambda - 1} \in \bar{\mathbb{Q}}_p$ is a root of unit of order $p^\lambda - 1$ (notice that D_λ is the ring of integers of the unramified extension of $\mathbb{Q}_p$ of degree λ).

We can prove that $\mathfrak{m}$ is a D_λ-module. Being D_λ a DVR, we have

$$\mathfrak{m} \cong \bigoplus_{i=1}^{n} D_\lambda / p^{a_i} D_\lambda \cong (\bigoplus_{i=1}^{n} \mathbb{Z}/p^{a_i}\mathbb{Z})^\lambda,$$

where the first is an isomorphism of D_λ-modules and the second as groups. □

Generalizing FCC12 and Bac15

$\mathfrak{m} = P^\lambda$: [FCC12] applies only when $\text{rank} P^\lambda = \lambda \text{rank} P < p - 1$.

For $\lambda \geq p - 1$ [FCC12] gives NO information on $1 + \mathfrak{m}$.

Theorem (idc)

Let p be a prime number, and let D be a PID such that p is a prime in D.

Let $(N, +)$ is a D-module of order a power of p, with $\mathrm{rank_D N < p - 1}$,

Then if $(N, +, \circ)$ is a "brace" then each element has the same order in $(N, +)$ and $(N, \circ)$.

In particular, if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$.

Here $\mathrm{rank_D N} = \#$summand of the dec. of N as a sum of cyclic $D-$mod.

[Bac15] gives the same result of last theorem for $D = \mathbb{Z}$.
Further examples: $D =$ the ring of integers of unramified extensions of $\mathbb{Q}_p$.
The theorem above admits a partial generalization to the case when D is a generic Dedekind domain, without any assumption on the factorization of pD. Here with "brace" we intend a two sided (+ some other) braces.

Generalization to Dedekind domanis

Theorem (idc)

Let $(N, +, \circ)$ be a two-sided (or also more general) brace of cardinality the power of a prime p.

Assume that $(N, +)$ is a $\mathcal{O}$-module, where $\mathcal{O}$ is the ring of integers of a number field or a p-adic field.

Let $p\mathcal{O} = P_1^{e_1} \cdots P_r^{e_r}$ be the factorization of $p\mathcal{O}$. For each $i = 1, \ldots, r$, let $f_i = [\frac{\mathcal{O}}{P_i} : \frac{\mathbb{Z}}{p\mathbb{Z}}]$ and denote by N_i the P_i-component of N.

If the $\mathbb{Z}$-rank of the abelian group N_i is $< f_i(p-1)$, for all $i = 1, \ldots, r$, then $(N, +)$ and $(N, \circ)$ have the same number of element of each order. In particular, if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$.

The case of small rank: char(A)>0

Theorem (idc)

Let $(A, \mathfrak{m})$ be a finite local ring with residue field of cardinality p^λ.

If rank $\mathfrak{m} < \lambda(p-1)$, then

$$A^* \cong \mathbb{F}_{p^\lambda}^* \times P^\lambda$$

where P is an abelian p-group.

Sketch of the proof. The condition $\lambda(p-1) > \text{rank}\ \mathfrak{m} = \lambda \text{rank}_{D_\lambda} \mathfrak{m}$ gives

$$\text{rank}_{D_\lambda} \mathfrak{m} < p - 1$$

therefore the previous theorem applies giving $1 + \mathfrak{m} \cong \mathfrak{m}$. Since $\mathfrak{m} = P^\lambda$ for some P, we can conclude. □

We have a classification of all small finite abelian groups occurring as group of units of a finite ring.

The case of small rank: char(A)=0

Let A a type 2 ring with $\epsilon = 2$.

Then, $\mathfrak{N}$ is a $\mathbb{Z}[i]$-module.

In this case we say that an abelian group H is *small* if

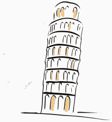
$$\mathrm{rank}(H_p) < 2(p-1), \text{ for all } p \equiv 3 \pmod 4.$$

Theorem (idc)

Let H be a small abelian group of odd order.

The group $\mathbb{Z}/4\mathbb{Z} \times H$, is the group of units of type 2 ring, if and only if H_p is the square of a group, $\forall p \equiv 3 \pmod 4$.

Thank you!



Bibliorgaphy

- Del Corso Ilaria, Dvornicich Roberto, Finite groups of units of finite characteristic rings, *Annali di Matematica Pura ed Applicata*, **197(3)** (2018), 661-671 .
- Del Corso Ilaria, Dvornicich Roberto, On Fuchs' Problem about the group of units of a ring, *Bull. London Math. Soc.*, **50** (2018,) 274-292.
- Del Corso Ilaria, Finitely generated abelian groups of units, *J. London Math. Soc.*, 101 (1) (2020), 247-270.
- Caranti A. Del Corso I., On the ranks of the additive and the multiplicative groups of a brace, *Rivista Mat. Univ. Parma*, *Special issue In honour of Roberto Dvornicich's 70th birthday.*
- Del Corso Ilaria, On Fuchs' problem on the group of units of a ring: the case of groups of *small* rank, *work in progress.*