Classification of finite rings

Jean-Claude Evard
Independent researcher

Back to my top RG-page:
https://www.researchgate.net/profile/Jean_Claude_Evard
List of links to my other RG-documents:
https://www.researchgate.net/publication/325593134_Links_to_my_RG_pages
Do you have any comment on anything posted on my RG Web site?
https://www.researchgate.net/post/Do_you_have_any_comment_on_anything_posted_on_my_RG_Web_site

Notes on the Classification of finite rings

Document created on June 1, 2018
Most recent update: June 20, 2018

Related documents:

Rings of prime order:
https://www.researchgate.net/publication/325793879_Rings_of_prime_order
List of publications on finite rings:
https://www.researchgate.net/publication/325531237_Publications_on_finite_rings
What is the best publication on the classification of finite rings?
https://www.researchgate.net/post/What_is_the_best_publication_on_the_classification_of_finite_rings
How many rings have pqr elements?
https://www.researchgate.net/post/How_many_rings_have_pqr_elements

Some terminology and notation

As usual, the word "ring" in mathematics is very different
from the word "ring" in English.
A possible reason why at the origin of the theory of rings, around 1870,
some mathematicians have chosen this word may be that in mathematics,
the additive part of a finite ring is a finite abelian group,
and every finite abelian group is isomorphic
to a direct sum of cyclic subgroups of prime power order:
https://en.wikipedia.org/wiki/Abelian_group
https://en.wikipedia.org/wiki/Abelian_group#Classification
https://en.wikipedia.org/wiki/Cyclic_group
http://mathworld.wolfram.com/CyclicGroup.html

Recall that a ring is a set provided with two operations,
one operation that looks like the ordinary addition of numbers,
the other that looks like the ordinary multiplication of numbers.
The two operations are connected
by the left and right distributivity
of the multiplication with respect to the addition:
https://en.wikipedia.org/wiki/Ring_(mathematics)
https://en.wikipedia.org/wiki/Distributive_property
https://en.wikipedia.org/wiki/File:Illustration_of_distributive_property_with_rectangles.svg

There has been a long struggle to decide
whether a multiplicative identity element
should be included in the definition of rings in mathematics.
Now, there is an agreement in the mathematical community
that it should be included.
It has also been decided that if we remove the condition
of having such an identity element i,
then we remove the letter i from the word "ring",
and we get the word "rng" or "RGN" in capital letters.
https://en.wikipedia.org/wiki/Ring_(mathematics)

https://en.wikipedia.org/wiki/Rng_(algebra)
I propose that in the case where the similar concept of "ring"
may have or not have a multiplicative identity element i,
I replace the letter i by the letter y,
as the letter y does not look like an identity:

1. Terminology
A ryng may have or not have an identity element.
A ring is a ryng with a multiplicative identity element i.
A rng is a ryng without multiplicative identity element i.

In the definition of a ryng R, we have that
the set R provided with the additive operation
forms a commutative group:
https://en.wikipedia.org/wiki/Group_(mathematics)
https://en.wikipedia.org/wiki/Abelian_group

In the definition of a ryng R, we have that
the set R provided with the multiplicative operation
forms a semigroup.
A semigroup is a set provided with a binary operation
that is associative:
https://en.wikipedia.org/wiki/Semigroup
https://en.wikipedia.org/wiki/Associative_property

In mathematics, to construct a ring, it is not sufficient to choose
an arbitrary abelian group for the addition
and an arbitrary semigroup for the multiplication.
The main difficulty is to have these two parts connected
by the property of **distributivity**.

It is like a large city located on two sides of a river,
and connected by only one bridge named **"Distributivity"**.

For any positive integer k, we will use the following notation:

a(k) = [The number of ryngs with k elements] .

The sequence (a(1), a(2), a(3), …) is called "Sequence A027623"
in the On-Line Encyclopedia of Integer Sequences:
https://oeis.org/wiki/Main_Page
https://oeis.org/A027623

Some pieces of information posted on the Internet
The following results are posted on the Internet:
https://en.wikipedia.org/wiki/Finite_ring
https://en.wikipedia.org/wiki/Finite_ring#Enumeration
I will try to find the references to the articles where they were first published.
On June 11, 2018, Issam Kaddoura posted the best summary
of results obtained so far about the sequence a(n):
https://www.researchgate.net/post/How_many_rings_have_pqr_elements#view=5b1ea229e5d99ecc2e3672b9
I will try to find the references to the articles where they were first published.

Here is a rewriting of all this:

Given distinct primes p and q, we have:

$a(p) = 2$ $a(p^2) = 11$ $a(pq)=4$ $a(p^2q) = 22$.

$a(2^3) = 52$ If $p > 2$, then $a(p^3) = 50+3p$ $a(2^4) = 390$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a(n)	1	2	2	11	2	4	2	52	11	4	2	22	2	4	4	390

n	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
a(n)	2	22	2	22	2	4	2	?	11	4	59	22	2	?	2	?

A conjecture posted by Peter Breuer

In his fourth posting of June 12, 2018,
https://www.researchgate.net/post/How_many_rings_have_pqr_elements#view=5b1f73bbeb87032f33451da4
Peter Breuer conjectured that
the function a(n) is multiplicative,
that is, $a(1) = 1$,
and for every positive integers x and y such that gcd(x, y) = 1,
we have a(xy) = a(x)a(y).
https://en.wikipedia.org/wiki/Multiplicative_function

Consequences of this conjecture

If this conjecture can be proved, then we could deduce from some of the above properties that,
if p, q, and r are distinct primes,
and if e, f, and g are positive integers, then

$a(p^eq^f) = a(p^e)a(q^f)$,
$a(p^eq^fr^g) = a(p^e)a(q^f)a(r^g)$,

in particular:

$a(pq) = a(p)a(q) = 2 \times 2 = 4$,
$a(pqr) = a(p)a(q)a(r) = 2 \times 2 \times 2 = 8$,
$a(p^2q) = a(p^2)a(q) = 11 \times 2 = 22$,

and then:

$a(24) = a(3\cdot 8) = a(3\cdot 2^3) = a(3)\cdot a(2^3) = 2\cdot 52 = 104$,
$a(30) = a(2\cdot 3\cdot 5) = a(2)\cdot a(3)\cdot a(5) = 2\cdot 2\cdot 2 = 8$.

Results published by Benjamin Fine in 1993

The article [BF, 1993] published by Benjamin Fine in 1993
https://www.researchgate.net/publication/325531237_Publications_on_finite_rings
https://www.maa.org/sites/default/files/Classification_of_Finite-Fine04025.pdf
contains the following results:

THEOREM 1. The number of rings R, up to isomorphism,
with cyclic additive group C_m is given by the number of divisors of m.
In particular, for each divisor d of m
there is a ring $R_d = \langle g;\, mg = 0,\, g^2 = dg \rangle$,
where g is an additive generator of C_m.
For different d's these rings are non-isomorphic.

For an abelian group G,
we let G(0) denote the ring with additive group G
and trivial multiplication.

COROLLARY 1. If p is a prime there are, up to isomorphism,
exactly two rings of order p, namely Z_P and $C_p(0)$.

COROLLARY 2. If p and q are distinct primes there are,
up to isomorphism, exactly four rings of order pq.
These are $\mathbf{Z}_{pq}$, $C_{pq}(0)$, $C_p(0) + \mathbf{Z}_q$, and $\mathbf{Z}_p + C_q(0)$.

COROLLARY 3. If $n = p_1 \ldots p_k$ is a square-free positive integer
with k distinct prime divisors
then there are, up to isomorphism, exactly 2^k rings of order n.

THEOREM 2. For any prime p there are, up to isomorphism,
exactly 11 rings of order p^2.

First remarks about counting finite r(i)ngs

Remark 1.

Let R be a r(i)ng.
Let x be an element of R.
Then **$0 \cdot x = 0$ and $x \cdot 0 = 0$**,
where $0 \cdot x$ means 0 times x and $x \cdot 0$ means x times 0.

Proof.

(1) By definition of the additive identity 0, we have $x \cdot 0 = x \cdot 0 + 0$.

(2) By definition of the additive inverse $(-(x \cdot 0))$, we have $0 = x \cdot 0 + (-x \cdot 0)$,
which implies that $x \cdot 0 + 0 = x \cdot 0 + (x \cdot 0 + (-x \cdot 0))$.

(3) By associativity of addition, we have
$x \cdot 0 + (x \cdot 0 + (-x \cdot 0)) = (x \cdot 0 + x \cdot 0) + (-x \cdot 0)$.

(4) By distributivity of multiplication with respect to addition,
we have $x \cdot 0 + x \cdot 0 = x \cdot (0 + 0)$,
which implies that $(x \cdot 0 + x \cdot 0) + (-(x \cdot 0)) = x \cdot (0 + 0) + (-(x \cdot 0))$.

(5) By definition of 0, we have $0 + 0 = 0$,
which implies that $x \cdot (0 + 0) + (-(x \cdot 0)) = x \cdot 0 + (-(x \cdot 0))$.

(6) By definition of the additive inverse $(-(x \cdot 0))$, we have $x \cdot 0 + (-(x \cdot 0)) = 0$.

It follows that:

(1) $x \cdot 0 = x \cdot 0 + 0$

(2) $\quad = x \cdot 0 + [x \cdot 0 + (-(x \cdot 0))]$

(3) $\quad = (x \cdot 0 + x \cdot 0) + (-(x \cdot 0))$

(4) $\quad = x \cdot (0 + 0) + (-(x \cdot 0))$

(5) $\quad = x \cdot 0 + (-(x \cdot 0))$,

(6) $\quad = 0$,

which implies that $x \cdot 0 = 0$.

In all this, we have not used any multiplicative identity element.
Consequently, the proof is valid in both rngs and rings, that is, in r(i)ngs.
The proof that $0 \cdot x = 0$ is almost identical, and I omit it (Boo).

Remark 2.

When a ring R has more than one element, then 1 is different from 0:

Let us prove this by contradiction:
Suppose that $1 = 0$.
Since R has more than one element, there exists at least one element x different from 0.
Then, by definition of 1, we have $x = 1x$.
The hypothesis $1 = 0$, implies that $1x = 0x$.
By Remark 1, we have $0x = 0$.
Thus $x = 1x = 0x = 0$, which implies that $x = 0$,
which contradicts the choice of x as a nonzero element.

Remark 3.

Given any abelian group G, we can construct a trivial r(i)ng R that has the set G has its set of elements, the group G has its additive commutative group, and that has the trivial operation of multiplication where every product of two elements of G is equal to zero. Let us denote this multiplication by MZ: Multiplication Zero.
Then the condition of associativity is trivially satisfied:
For all x, y, z in R, we have $(xy)z = 0z = 0$ by Remark 1.
And we have $x(yz) = x0 = 0$ also by remark 1.

The conditions of distributivity are also satisfied:
$x(y + z) = 0$ by definition of MZ.
$xy + xz = 0 + 0 = 0$, also by definition of MZ.
It follows that $x(y + z) = 0 = xy + xz$.

The proof that $(x + y)z = xz + yz$ is almost identical.

Let us denote this ryng by MZ(G), that is,
MZ(G) is the ryng that has additive group G and Multiplication Zero.

Remark 4.

When G = {0}, the ryng is a ring: MG(G) = {0} is a ring with identity $1 = 0$.

Remark 5.

If G is an abelian group with more than one element, then MZ(G) is a rng.

Let us prove this by contradiction.
Suppose that the r(i)ng MZ(G) is not a rng so that it is a ring, and it has a multiplicative identity 1.
This implies by Remark 2 that 1 is not equal to 0.
By definition of the multiplicative identity, we have $1 = 1 \times 1$.
By definition of MZ, we have $1 \times 1 = 0$.
It follows that $1 = 1 \times 1 = 0$, which implies that $1 = 0$, which contradicts the above assertion that 1 is not equal to 0.

R(i)ng R with a prime number p of elements.
Because |R| = p is prime, the additive group of R is cyclic.
Because for every prime p any two cyclic groups are isomorphic,
they are all isomorphic to the cyclic group Cp = Zp
http://mathworld.wolfram.com/CyclicGroup.html
There are only two r(i)ngs of order p: MG(Cp) and Fp.
http://www.uio.no/studier/emner/matnat/math/MAT2200/v15/smallrings.pdf
http://mathworld.wolfram.com/FiniteField.html

Rings of prime order

See my document **"Rings of prime order":**
https://www.researchgate.net/publication/325793879_Rings_of_prime_order

Under construction

The following Web page of Wikipedia contains a lot of wonderful information about finite rings:
https://en.wikipedia.org/wiki/Finite_ring
https://en.wikipedia.org/wiki/Finite_ring#Enumeration

The following Web page contains information about results obtained by students of Gregory Dresden on finite r(i)ngs:
https://web.archive.org/web/20170501203914/http://home.wlu.edu/~dresdeng/smallrings/
http://dresden.academic.wlu.edu/

Recall that a **domain D** is a nonzero ring such that
for all pairs of elements a and b of D such that ab = 0,
we have that a = 0 or b = 0.
https://en.wikipedia.org/wiki/Domain_(ring_theory)

Wedderburn's little theorem: Every finite domain is a field.
https://en.wikipedia.org/wiki/Wedderburn%27s_little_theorem
https://en.wikipedia.org/wiki/Joseph_Wedderburn

Wedderburn's theorem:
Every finite division ring is commutative.
Equivalently:
If every nonzero element r of a finite ring R has a multiplicative inverse, then R is commutative.

Equivalently:
If every nonzero element r of a finite ring R has a multiplicative inverse, then R is commutative.
https://en.wikipedia.org/wiki/Finite_ring#Wedderburn's_theorems
https://en.wikipedia.org/wiki/Joseph_Wedderburn

Theorem (Wedderburn). If A is a simple ring with unit 1
and A possesses a minimal left ideal I,
then A is isomorphic to the ring of n × n-matrices over a division ring.
https://en.wikipedia.org/wiki/Simple_ring
https://en.wikipedia.org/wiki/Minimal_ideal
https://en.wikipedia.org/wiki/Division_ring
https://en.wikipedia.org/wiki/Joseph_Wedderburn

For readers who are not specialized in ring theory, to understand the pieces of information that I am presenting below, it is important to know that experts in ring theory navigate all the time between rings and associative algebras over a ring. Sometimes, they prefer to think in terms of rings, and some other times, they prefer to think in terms of associative algebras over a ring.

A ring has 2 operations: Addition and multiplication.

An algebra A over a ring R has 3 “operations”: The above two, and multiplication of any element a of the algebra A by any element r of the ring R.
In non-commutative cases, ra is not equal to ar. We have left multiplication and right multiplication.

I write “operation” between quote marks, because the first two operations are internal: We multiply inside the algebra. The third one is external: We multiply an element a inside the algebra A by an element r outside the algebra A, and the results ra and ar are inside the algebra A.
https://en.wikipedia.org/wiki/Associative_algebra
https://en.wikipedia.org/wiki/Associative_algebra#Examples
https://en.wikipedia.org/wiki/Matrix_ring
https://mathoverflow.net/questions/21899/definition-of-an-algebra-over-a-noncommutative-ring
https://math.stackexchange.com/questions/380177/difference-between-ring-and-algebra
https://math.stackexchange.com/questions/53507/algebra-over-a-ring

In 1907, Joseph Wedderburn published what is perhaps his most famous article on the classification of semisimple algebras. In this paper “On hypercomplex numbers”, which appeared in the Proceedings of the London Mathematical Society, he showed that every semisimple algebra is a direct sum of simple algebras and that a simple algebra is a matrix algebra over a division ring.
http://www-history.mcs.st-andrews.ac.uk/Biographies/Wedderburn.html
https://en.wikipedia.org/wiki/Simple_ring
https://en.wikipedia.org/wiki/Semisimple_algebra
https://en.wikipedia.org/wiki/Matrix_ring
https://en.wikipedia.org/wiki/Joseph_Wedderburn

In 1908, Josheph Wedderburn had the important idea of splitting the study of a ring into two parts, one part he called the radical, the part which was left being called semi-simple. He used matrix rings to classify the semi-simple part. The importance of this work can be seen from the fact that the next 56 years were spent generalizing it.

We should point out that Joseph did not prove his results for rings but rather for hypercomplex systems - a term no longer in use which meant a finite dimensional algebra over a field.

The Wedderburn theory was extended to non-commutative rings satisfying both ascending and descending finiteness conditions (called chain conditions) by Artin in 1927. It was not until 1939 that Hopkins showed that only the descending chain condition was necessary.
http://www-history.mcs.st-andrews.ac.uk/HistTopics/Ring_theory.html
http://www-history.mcs.st-andrews.ac.uk/HistTopics/Ring_theory.html#s43

Artin–Wedderburn theorem: Any Artinian semi-simple ring R is isomorphic to a product of finitely many n_i-by-n_i matrix rings over division rings D_i, for some integers n_i, both of which are uniquely determined up to permutation of the index i.
https://en.wikipedia.org/wiki/Artin–Wedderburn_theorem
https://en.wikipedia.org/wiki/Semisimple_module#Semisimple_rings

Additional information:

https://math.stackexchange.com/questions/368323/structure-theorem-of-finite-rings
https://math.stackexchange.com/questions/44277/rings-and-modules-of-finite-order?rq=1
https://math.stackexchange.com/questions/368323/structure-theorem-of-finite-rings?noredirect=1&lq=1
https://www.sciencedirect.com/search?qs=finite+rings&origin=article&zone=qSearch
https://www.hindawi.com/journals/jmath/2013/467905/

Mathematicians working on finite rings:

Alexei Miasnikov, Distinguished Professor
Stevens Institute of Technology
Algebra and foundations of mathematics
https://www.researchgate.net/profile/Alexei_Miasnikov

Under construction

Credits to the answerers to my question

On June 11, 2018, Issam Kaddoura posted the best summary of results obtained so far about the sequence a(n):
https://www.researchgate.net/post/How_many_rings_have_pqr_elements#view=5b1ea229e5d99ecc2e3672b9

Under construction

End of this document