mathoverflow

Classification of finite commutative rings

Asked 14 years, 1 month ago Modified 8 years, 1 month ago Viewed 11k times

41

Is there a classification of finite commutative rings available? If not, what are the best structure theorem that are known at present? All I know is a result that every finite commutative ring is a direct product of local commutative rings (this is correct, right?) in some paper which computes the size of the general linear group over that ring.

ac.commutative-algebra

Share Cite Improve this question Follow

asked Nov 29, 2009 at 13:22

Purațci Vinnani

6 I'd guess you know this already, but Wedderburn's little theorem provides a nice dichotomy (every finite commutative ring is either a field or has zero divisors) although it's far from a complete structure theorem. – Harrison Brown Nov 29, 2009 at 19:32

Some progress has been made: doi.org/10.2140/involve.2023.16.151 – Thrash Jun 18, 2023 at 21:22

4 Answers

Sorted by: Highest score (default)

17

Yes, a finite ring R is a finite direct sum of local finite rings. As a first step, for each prime p there is a subring R_p of R corresponding to the elements annihilated by the powers of p. ~~R_p is then an algebra over $\mathbb{Z}/p$.~~ R_p then resembles an algebra over $\mathbb{Z}/p$ and it could be one, but it can also have a more complicated structure as an abelian p-group (see below). This step generalizes to maximal ideals: For each maximal ideal m, R_m is the subring of elements annihilated by m^n for some n, and R is the direct sum of these subrings, which are local rings.

It is not difficult to write down a rough partial classification of of local finite rings. If R is local with maximal ideal m, it ~~is~~ resembles an algebra over the finite field $F = R/m$; the associated graded ring is such an algebra. If you choose a basis $x_1, \dots, x_n$ for m/m^2, then R or its associated graded is a quotient of the polynomial ring $F[\vec{x}]$ in which only finitely many monomials are non-zero. You can make a diagram of these non-zero monomials; they can be any order ideal in the n-dimensional orthant. Or, in basis-independent form, R has a length, which is the largest nonvanishing power of m, and each m^k/m^{k+1} is some quotient of the kth symmetric power of the generating vector space $V = m/m^2$.

After that, the non-zero monomials may be linearly dependent (and never mind that R might be more complicated than its associated graded). Informally, there will be an endless stream of partial results and there will never be a complete classification when the length of the local ring is 3 or more. To see this, suppose that $m^4 = 0$, and suppose that m^3 is only one dimension shy of $S^3(V)$. Then the ring is defined by an arbitrary symmetric trilinear form in V. These make a "wild" sequence of algebraic varieties, in the same sense that people say that the representation theories of certain rings are wild. For instance, I think (not quite sure) that it is NP-hard to determine when two such trilinear forms are equivalent. NP-hardness is not by itself rigorously equivalent to no classification, but informally the classification is an intractable mess.

If the nonvanishing monomials in R are linearly independent, then it is a toric local ring. Toric local rings are certainly a tractable class of finite rings.

The situation is similar to non-commutative p-groups, which are also wild and will never be classified. In both cases, certain classes have a nice structure. It is also interesting to make estimates for how many there are.

Note: Corrected per comment.

Share Cite Improve this answer Follow

edited Nov 28, 2015 at 14:46
Matemáticos Chibchas

answered Nov 29, 2009 at 17:44
Greg Kuperberg

3 These two assertions: "R_p is then an algebra over Z/p." and "If R is local with maximal ideal m, it is an algebra over the finite field F=R/m." -- are obviously wrong, as applied to finite rings, in general. Take R = R_p = R_m = Z/p^nZ, n>1. – Leonid Positselski Nov 29, 2009 at 18:23

Oh blech, I forgot all about non-split extensions. Thank you for that correction. – Greg Kuperberg Nov 29, 2009 at 18:53

20

This is a very interesting question related to the Hilbert scheme $Hilb^n(\mathbb{A}^d)$ classifying n points in affine space $\mathbb{A}^d$. I don't think there is a classification but there is an estimate for the number of commutative rings of order $\leq N$. It is

$$exp[\frac{2}{27}\frac{log(N)^3}{(log2)^2} + O(log(N)^{\frac{8}{3}})] \quad forN \rightarrow \infty$$

The proof of this result due to Bjorn Poonen and of many related interesting theorems is in his article

You will also find astonishing conjectures in the article like:

The fraction of local rings of order $\leq N$ among all commutative rings A of order $\leq N$ tends to 1. Same limit 1 for the fraction of rings "of characteristic 8" in the sense that $8.\,1_A = 0$ but $4.1_A \neq 0$.

Share Cite Improve this answer Follow

edited Jan 5, 2010 at 9:17

answered Nov 29, 2009 at 15:32

Georges Elencwajg

11

The characterization of Artinian rings is relevant of course. See also the book "Finite commutative rings and their applications" and this web page.

Share Cite Improve this answer Follow

edited Nov 29, 2009 at 14:26

answered Nov 29, 2009 at 13:57

lhf

6

As always one should check out the OEIS for questions of this type. In this case see http://oeis.org/A027623

Share Cite Improve this answer Follow

answered Dec 1, 2010 at 6:22

Edwin Clark

4 Rather see oeis.org/A037289 which is specific to commutative rings. – Charles Jul 10, 2012 at 13:38

3 Or even see oeis.org/A127707 which is specific to commutative *unital* rings. – Watson Apr 28, 2021 at 17:43