comput. complex. **15** (2007), 342–390
1016-3328/07/040342-49
DOI 10.1007/s00037-007-0219-8

© Birkhäuser Verlag, Basel 2007

computational complexity

COMPLEXITY OF RING MORPHISM PROBLEMS

Neeraj Kayal and Nitin Saxena

Abstract. We study the complexity of the isomorphism and automorphism problems for finite rings. We show that both integer factorization and graph isomorphism reduce to the problem of counting automorphisms of a ring. This counting problem is shown to be in the functional version of the complexity class AM $\cap$ coAM and hence is not NP-complete unless the polynomial hierarchy collapses. As a "positive" result we show that deciding whether a given ring has a non-trivial automorphism can be done in deterministic polynomial time. Finding such an automorphism is, however, shown to be randomly equivalent to integer factorization.

Keywords. Ring, isomorphism, automorphism, polynomial hierarchy, graph isomorphism, integer factorization.
Subject classification. 68Q15, 13P99.

1. Introduction

A *ring* consists of a set of elements together with addition and multiplication operations. These structures are fundamental objects of study in mathematics and particularly so in algebra and number theory. It has long been recognized that the group of automorphisms of a ring provides valuable information about the structure of the ring. Galois (1846) initiated the study of the group of automorphisms of a field and it was later applied by Abel (Rosen 1995) to prove the celebrated theorem that there does not exist any formula for finding the roots of a quintic (degree 5) polynomial. However, to the best of our knowledge, the computational complexity of the ring isomorphism and automorphism related problems has not been investigated so far. In this paper, we initiate such a study and show interesting connections to some well known problems.

We will restrict our attention to finite rings with unity. We assume that the rings are given in terms of the *basis* of their additive group and the multiplication table of basis elements. Given two rings in this form, the *ring isomorphism* problem is to test if the rings are isomorphic. We show that this problem is in

$\mathrm{NP} \cap \mathrm{coAM}$ and is at least as hard as the graph isomorphism problem. Thus, ring isomorphism is a natural algebraic problem whose complexity status is similar to that of graph isomorphism. The search version of the isomorphism problem is to *find an isomorphism* between two given rings. We show that integer factoring reduces to the search version of the problem.

Another variant of the problem is to *count the number of isomorphisms* between two rings. We show that both integer factorization and graph isomorphism reduce to this problem. We also show that this problem is equivalent to that of counting the number of automorphisms in a ring and lies in the class $\mathrm{FP}^{\mathrm{AM}\cap\mathrm{coAM}}$. This implies that the problem is not NP-hard unless the polynomial hierarchy collapses to Σ_2 (Schöning 1988).

The *ring automorphism* problem is to test if a ring has a non-trivial automorphism. We prove that this problem is in P. This is in contrast to the corresponding problem for graphs whose status is still open. On the other hand we show that the problem of *finding a nontrivial automorphism* of a given ring is equivalent to integer factoring. This implies that the search version of the problem is likely to be strictly harder than the decision version. We also show a connection of polynomial factorization to finding a nontrivial automorphism of a ring.

The most general problem here is to *compute the automorphism group* of a given ring, in terms of a small set of generators. It is easy to see that all the above problems reduce to it. Also, the proof of upper bound on counting automorphisms can be adapted to exhibit an AM protocol for it implying that this problem too is not NP-hard unless $\mathrm{PH} = \Sigma_2^P$.

We start with a warm up of groups, rings and complexity theory notions in Sections 2 and 3. We present upper and lower bounds on the complexity of Ring Isomorphism, Counting Ring Automorphisms, finding a Ring Isomorphism, deciding Ring Automorphism and finding a nontrivial Ring Automorphism in the subsequent sections respectively. Some basic structural properties of rings can be found in the Appendix together with brief proofs.

The reduction from Graph Isomorphism to Ring Isomorphism given in this paper was improved by Agrawal & Saxena (2005, 2006). Using the new reduction they were able to prove that Graph Isomorphism can also be reduced to the problem of Cubic Forms Equivalence.

2. Basics of groups and rings

In this section we give the basics of rings, see the appendix for more details. A *group* is a set of elements with a suitably defined operation of multiplication while a *ring* is a set of elements with two operations of addition $(+)$ and multiplication $(\cdot)$ defined. There are two useful groups living in a ring R. Firstly, $(R, +)$ is a group with respect to addition called the *additive group*. If R^* is the set of elements in R having multiplicative inverses then $(R^*, \cdot)$ is the second group called the *multiplicative group*.

2.1. Representing rings. For concreteness we first fix the way we are going to present the finite rings and their homomorphisms in the input or the output.

DEFINITION 2.1. **Basis representation of rings:** *A finite ring R is given by first describing its additive group in terms of n additive generators and then specifying multiplication by giving for each pair of generators, their product as an element of the additive group. More concretely, R is presented as:*

$$(R, +, .) := \langle (d_1, d_2, d_3, \ldots, d_n), ((a_{i,j,k}))_{1 \le i,j,k \le n} \rangle ,$$

where, for all $1 \le i, j, k \le n$, $0 \le a_{i,j,k} < d_k$ and $a_{i,j,k} \in \mathbb{Z}$.

This specifies a ring R generated by n elements $b_1, b_2, \ldots b_n$ with each b_i having additive order d_i and $(R, +) = (\mathbb{Z}/d_1\mathbb{Z})b_1 \oplus (\mathbb{Z}/d_2\mathbb{Z})b_2 \cdots \oplus (\mathbb{Z}/d_n\mathbb{Z})b_n$. Moreover, multiplication in R is defined by specifying the product of each pair of generators as an integer linear combination of the generators: for $1 \le i, j \le n$, $b_i \cdot b_j = \sum_{k=1}^{n} a_{i,j,k} b_k$.

DEFINITION 2.2. **Representation of maps on rings:** *Suppose R_1 is a ring given in terms of its additive generators $b_1, \ldots, b_n$ and ring R_2 given in terms of $c_1, \ldots, c_n$. In this paper maps on rings would invariably be homomorphisms on the additive group. Then to specify any map $\phi : R_1 \to R_2$, it is enough to give the images $\phi(b_1), \ldots, \phi(b_n)$. So we represent ϕ by an $n \times n$ matrix of integers A, such that for all $1 \le i \le n$:*

$$\phi(b_i) = \sum_{j=1}^{n} A_{ij} c_j$$

and for all $1 \le i, j \le n$, $0 \le A_{ij} <$ additive order of c_j.

EXAMPLE 2.3. Consider the ring $R := (\mathbb{Z}/3\mathbb{Z})[x]/(x^2 - x + 1)$. Here, 1 and x can be taken as basis elements and $(R, +) = (\mathbb{Z}/3\mathbb{Z}) \cdot 1 \oplus (\mathbb{Z}/3\mathbb{Z}) \cdot x$. Multiplication on the basis elements is defined as: $1 \cdot 1 = 1 \cdot 1 + 0 \cdot x$, $x \cdot 1 = 1 \cdot x = 0 \cdot 1 + 1 \cdot x$ and $x \cdot x = 2 \cdot 1 + 1 \cdot x$. Note that the map ϕ sending $1 \mapsto 1$ and $x \mapsto -1$ is a homomorphism from R to itself and wrt to the basis $1, x$ it can be represented as: $A = \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}$. ◊

2.2. The problems. Firstly, we define the ring isomorphism and related problems that we are going to explore.

- The *ring isomorphism problem* is to decide whether two given rings are isomorphic. The corresponding language we define as:
$$\mathrm{RI} := \big\{(R_1, R_2) \mid \text{ rings } R_1, R_2 \text{ are given in the basis representation and } R_1 \cong R_2\big\}\,.$$
- Given two rings $R_1,\ R_2$ in basis form, FRI is the functional problem of *computing an isomorphism* from $R_1 \to R_2$ (if one exists).
- #RI is defined as the functional problem of *computing the number of isomorphisms* between two rings given in basis form.
- RA is defined as the problem of deciding whether a given ring has a *nontrivial ring automorphism.* The corresponding language is:
$$\mathrm{RA} := \big\{R \mid R \text{ is a ring in basis form s.t. } \#Aut(R) > 1\big\}\,.$$
- FRA is the functionl problem of *computing a nontrivial automorphism* of a ring R given in the basis form.
- #RA is defined as the functional problem of *computing the number of automorphisms* of a given ring. Its decision version can be viewed as the language:
$$\mathrm{cRA} := \big\{(R, k) \mid R \text{ is a ring in basis form s.t. } \#Aut(R) \geq k\big\}\,. \tag{2.4}$$

2.3. The preliminaries. If G, H are two groups then we use $H \leq G$ to denote that H is a subgroup of G. If G is finite then the size of a subgroup of G divides $\#G$. A converse does not hold in general but if for a prime p, $p^k | \#G$ then there always exist a subgroup of size p^k. If p^k is the highest power of p dividing $\#G$ then a subgroup of size p^k is called a *p-Sylow subgroup* of G. A p-Sylow subgroup S_p of size p^k can be broken into a *composition series*, i.e., there are groups G_i of size p^{k-i} such that:
$$S_p = G_0 > G_1 > G_2 > \cdots > G_k = \{1\}\,.$$

In analysing a ring R we use special subsets of R called *ideals.*

Definition 2.5. *A subset $I \subseteq R$ is an* ideal *of R if:*

- $(I, +)$ *is a subgroup of* $(R, +)$, *and*
- *for all $i \in I,\ r \in R$, both $i \cdot r$ and $r \cdot i$ are in I. This can also be stated as: $\forall r \in R$ both $r \cdot I,\ I \cdot r \subseteq I$.*

Ideals can be multiplied together to give new (smaller) ideals.

Definition 2.6. *Let $\mathcal{I}, \mathcal{J}$ be two ideals of a ring R. We define their product as*

$$\mathcal{I} \cdot \mathcal{J} := \textit{ ring generated by the elements } \{ij \mid i \in \mathcal{I}, j \in \mathcal{J}\}\,.$$

Powering of ideals, $\mathcal{I}^t$ for positive integer t, is defined similarly. It is easy to see that $\mathcal{I} \cdot \mathcal{J}$ is again an ideal of R.

Algebraic structures mostly break into simpler objects. In the case of rings we get the following simpler rings.

Definition 2.7. **Indecomposable or local ring:** *A ring R is said to be indecomposable or local if there do not exist rings R_1, R_2 such that $R \cong R_1 \times R_2$, where $\times$ denotes the natural composition of two rings with component wise addition and multiplication.*

Commutative local rings have nice properties (see the appendix and the text McDonald 1974). For instance, if R is a commutative local ring then for all $r \in R$ either r is invertible or r is a *nilpotent*, i.e., $\exists k,\ r^k = 0$. This makes $\mathcal{M} := R \setminus R^*$ an ideal of R and it can be shown that $\mathcal{M}$ is the *unique maximal ideal* of R.

Example 2.8. Let $n = p^2 q$ where $p,\ q$ are distinct primes and define a natural ring $R := (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$. Then observe that R decomposes as $(\mathbb{Z}/p^2\mathbb{Z}, +, \cdot) \times (\mathbb{Z}/q\mathbb{Z}, +, \cdot)$ where the two *component* rings are local. $\Diamond$

Example 2.9. Consider a ring $R := \mathbb{F}[x, y]/(x^3, y^2)$. The subset yR, denoted as (y), is an ideal of R. Similarly, $xR + yR$, denoted by (x, y), is also an ideal of R. Note that the product of these two ideals is $(y) \cdot (x, y) = (xy, y^2) = (xy)$. Similarly in R, $(x, y)^2 = (x^2, xy),\ (x, y)^3 = (x^2 y)$ and $(x, y)^4 = 0$. Moreover, it can be shown that R is a local ring with $\mathcal{M} = (x, y)$ as its unique maximal ideal. $\Diamond$

Example 2.10. It is an interesting exercise to show that $R_1 := \mathbb{F}[x,y]/(x^3, y(x+y))$ is a nonzero local ring while $R_2 := \mathbb{F}(y)[x]/(x^3, y(x+y))$ is the zero ring. $\Diamond$

We collect some of the known results about rings. Their proofs can be found in algebra texts, for example Lang (1994); McDonald (1974).

There is a classification known for finite commutative groups. Basically, each such group completely decomposes into a bunch of *cyclic* groups.

Proposition 2.11 (Structure theorem for abelian groups). *If R is a finite ring then its additive group $(R,+)$ can be uniquely (up to permutations) expressed as:*

$$(R,+) \cong \bigoplus_i (\mathbb{Z}/{p_i}^{\alpha_i}\mathbb{Z}) \,,$$

where p_i's are primes (not necessarily distinct) and $\alpha_i \in \mathbb{Z}^{\geq 1}$.

Remark 2.12. *This theorem can be used to check in polynomial time whether for two rings, given in basis form, the additive groups are isomorphic or not. Suppose the two additive groups are $G := (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_n\mathbb{Z})$ and $G' := (\mathbb{Z}/d'_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d'_n\mathbb{Z})$. Consider the set $D = \{d_i \mid i \in [n]\} \cup \{d'_i \mid i \in [n]\}$. We take gcds of all pairs of integers from the set D and expand D in each such gcd-operation as: if $\alpha, \beta \in D$ have a nontrivial gcd then replace them by $\frac{\alpha}{gcd(\alpha,\beta)}$, $\frac{\beta}{gcd(\alpha,\beta)}$ and $gcd(\alpha,\beta)$. We can keep repeating this process on the new expanded D till all the elements of D become mutually coprime. It is guaranteed to stop in polynomial time, for D can expand to a maximum size of* $\log(\#G \cdot \#G')$ *as the number of prime factors of a number N are less than $\log N$. Now factor d_i 's and d'_j 's as much as possible using the numbers from D. Say, $d_i = d_{i,1}^{e_1} \ldots d_{i,k}^{e_k}$ where $d_{i,1}, \ldots, d_{i,k} \in D$ are mutually coprime. We can refine the decomposition of G by breaking $(\mathbb{Z}_{d_i}, +)$ as:*

$$(\mathbb{Z}/d_{i,1}^{e_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_{i,k}^{e_k}\mathbb{Z}) \,.$$

At the end of all this refining of d_i's and d'_j's using D, let the finer *structural decompositions be: $G \cong (\mathbb{Z}/m_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m_{n'}\mathbb{Z})$ and $G' \cong (\mathbb{Z}/m'_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m'_{n'}\mathbb{Z})$. Now by invoking the structure theorem: G will be isomorphic to G' if and only if the* multi-sets *(i.e., elements with repetition) $\{m_i\}_{i\in[n']}$ and $\{m'_i\}_{i\in[n']}$ are equal.*

Using the structure theorem of abelian groups, we can compute $\#Aut(R,+)$ of a ring R given in basis form and having a *prime-power* size.

Proposition 2.13. *Given a ring R in terms of additive generators, all having prime-power additive orders, we can compute the number of automorphisms of the additive group of R, $\#Aut(R,+)$, in polynomial time.*

Proof. Automorphisms of the additive group $(R,+)$ are nothing but the invertible linear maps on the additive generators of R. Thus, to compute $\#Aut(R,+)$ we compute the number of invertible linear maps or the number of invertible matrices.

Let $(R,+)$ be given as $\cong \bigoplus_{i=1}^{l} \bigoplus_{j} (\mathbb{Z}/{p_i}^{\alpha_{i,j}}\mathbb{Z})$, where p_i's are distinct primes and $\alpha_{i,j} \in \mathbb{Z}^{\geq 1}$. For $1 \leq i \leq l$ define subrings R_i of R as:

$$R_i := \{r \in R \mid r \text{ has power-of-}p_i \text{ additive order}\}\,.$$

Observe that

$$R \cong R_1 \times \cdots \times R_l\,;$$

this is because if $r_i \in R_i$ and $r_j \in R_j$ $(i \neq j)$ then for some $c_i, c_j \in \mathbb{Z}^{\geq 0}$, $p_i^{c_i} r_i r_j = p_j^{c_j} r_i r_j = 0$ which implies that $r_i r_j = 0$ (since $\exists a, b \in \mathbb{Z}$ such that $ap_i^{c_i} + bp_j^{c_j} = 1$) and by a similar argument $r_1 \in R_1, \ldots, r_l \in R_l$ are *linearly independent*.

This decomposition of R gives us:

$$\#Aut(R,+) = \prod_{i=1}^{l} \#Aut(R_i,+)\,.$$

Thus, it suffices to show how to compute $\#Aut(R,+)$ when $(R,+)$ is given as $\cong \bigoplus_{i=1}^{n} (\mathbb{Z}/p^{\alpha_i}\mathbb{Z})$ where p is a prime and $\alpha_i \in \mathbb{Z}^{\geq 1}$.

Suppose we are given R in terms of the following additive basis:

$$\begin{aligned}(R,+) = (\mathbb{Z}/p^{\beta_1}\mathbb{Z})e_{1,1} \oplus \cdots \oplus (\mathbb{Z}/p^{\beta_1}\mathbb{Z})e_{1,n_1} \oplus \cdots \\ \cdots \oplus (\mathbb{Z}/p^{\beta_m}\mathbb{Z})e_{m,1} \oplus \cdots \oplus (\mathbb{Z}/p^{\beta_m}\mathbb{Z})e_{m,n_m}\,,\end{aligned}$$

where $n_1 + \cdots + n_m = n$ and $1 \leq \beta_1 < \cdots < \beta_m$.

Observe that $\phi \in Aut(R,+)$ iff the matrix A describing the map ϕ is invertible (mod p) and preserves the additive orders of $e_{i,j}$'s. Our intention is to count the number of all such matrices A. To do that let us see how A looks:

$$A = \begin{pmatrix} B_{1,1} & B_{1,2} & \ldots & B_{1,m} \\ B_{2,1} & B_{2,2} & \ldots & B_{2,m} \\ \vdots & \ldots & \ddots & \vdots \\ B_{m,1} & B_{m,2} & \ldots & B_{m,m} \end{pmatrix}_{n \times n}$$

where the block matrices $B_{i,j}$'s are integer matrices of size $n_i \times n_j$. The properties of these block matrices which make A describe an automorphism of $(R,+)$ are:

- for $1 \le j < i \le m$: entries in B_{ij} are from $\{0,1,\ldots,p^{\beta_j}-1\}$,
- for $1 \le i \le m$: entries in B_{ii} are from $\{0,1,\ldots,p^{\beta_i}-1\}$ and B_{ii} is invertible (mod p),
- for $1 \le i < j \le m$: entries in B_{ij} are from $\{0,1,\ldots,p^{\beta_j}-1\}$ and $B_{ij} \equiv 0 \pmod{p^{\beta_j-\beta_i}}$.

It is not difficult to see that the number of matrices satisfying these conditions can be found in time polynomial in $(n_1\beta_1 + \cdots + n_m\beta_m)(\log p)$, and hence the number of A's which describe an automorphism of $(R,+)$. □

Remark 2.14. *When a ring R, given in basis form, is of composite size then computing $\#Aut(R,+)$ entails factoring integers. For example, suppose $n = pq$ where $p \neq q$ are primes and ring R is given as $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$. Then $\#Aut(R,+) = (p-1)(q-1) = \phi(n)$ and if we compute $\phi(n)$ then we can factorize n in randomized polynomial time (Miller 1976).*

Unlike commutative groups, a classification of commutative rings is not known yet. But as a first step rings can be decomposed uniquely into indecomposable rings.

Proposition 2.15 (Structure theorem for rings). *If R is a finite ring with unity then it can be uniquely (up to permutations) decomposed into indecomposable rings $R_1,\ldots,R_s$ such that*

$$R = R_1 \times \cdots \times R_s\,.$$

Remark 2.16. *In fact, for a* commutative *ring R its decomposition can be found in polynomial time given oracles to integer and polynomial factorizations (see McDonald 1974 and Lemma 9.6). Observe that any commutative ring R with characteristic n can be expressed as:*

$$R \;\cong\; (\mathbb{Z}/n\mathbb{Z})[x_1,\ldots,x_m]/\big(f_1(\overline{x}),\ldots,f_\ell(\overline{x})\big)\,,$$

where $\overline{x} = (x_1,x_2,\ldots,x_m)$ and $f_1,\ldots,f_\ell$ are polynomials in x_i's capturing the multiplicative relations in the ring R. The above expression hints that if we can factor n into its prime factors and polynomials into irreducible factors (over local rings) then we can effectively factor ring R into its indecomposable components.

Example 2.17. Consider the ring $R := (\mathbb{Z}/p^2q^3\mathbb{Z})[x,y]/(x^4, px, y^2 - y)$. By factoring the characteristic p^2q^3 we get:

$$R \cong (\mathbb{Z}/p^2\mathbb{Z})[x,y]/(x^4, px, y^2 - y) \times (\mathbb{Z}/q^3\mathbb{Z})[x,y]/(x^4, px, y^2 - y)\,.$$

Further, by factoring $y^2 - y$ into *coprime* irreducibles over the respective local rings in x we get:

$$\begin{aligned} R \cong\ & (\mathbb{Z}/p^2\mathbb{Z})[x,y]/(x^4, px, y) \times (\mathbb{Z}/p^2\mathbb{Z})[x,y]/(x^4, px, y-1) \\ & \times (\mathbb{Z}/q^3\mathbb{Z})[x,y]/(x^4, px, y) \times (\mathbb{Z}/q^3\mathbb{Z})[x,y]/(x^4, px, y-1)\,. \qquad \Diamond \end{aligned}$$

3. Basics of complexity theory

A decision problem in computer science is represented by a *language* $L \subseteq \{0,1\}^*$ which is the set of all 'yes' strings. We say that L is in the *complexity class* NP if there is a polynomial time deterministic Turing Machine M and a positive number c such that:

$$L = \left\{x \mid\ \exists y \in \{0,1\}^{|x|^c},\ M(x,y) \text{ accepts}\right\}.$$

x is the *input* and y is called as *witness*, *membership proof* or *nondeterministic guess*. L is said to be in coNP iff $\overline{L} \in$ NP.

Example 3.1. Consider the problem of satisfiability of boolean formulas:

$$\text{3-SAT} := \left\{\phi(x_1, \ldots, x_n) \mid \phi = \wedge_{i=1}^m (x_{i_1} \vee x_{i_2} \vee x_{i_3}) \text{ and has a satisfying assignment}\right\}.$$

3-SAT is in NP as given a formula ϕ and a satisfying assignment $\overline{v}$ it can be verified in polynomial time whether $\phi(\overline{v})$ is 'true'. $\Diamond$

We can also define a "randomized" version of the class NP called AM (for Arthur–Merlin protocol). We will say a language L is in AM if there is a positive number c and a polynomial time deterministic Turing Machine M such that:

$$\begin{aligned} x \in L &\Rightarrow \text{Prob}_{y \in \{0,1\}^{|x|^c}}\left[\exists z \in \{0,1\}^{|x|^c},\ M(x,y,z) \text{ accepts}\right] \geq \frac{2}{3}\,, \\ x \notin L &\Rightarrow \text{Prob}_{y \in \{0,1\}^{|x|^c}}\left[\exists z \in \{0,1\}^{|x|^c},\ M(x,y,z) \text{ accepts}\right] \leq \frac{1}{3}\,. \end{aligned}$$

Typically, the proof of showing an $L \in$ AM goes through by giving a protocol between the *Verifier* (named Arthur – the 'king') who can do randomized polynomial time computations and the *Prover* (named Merlin – the 'advisor' to the king) who has unlimited computational resources. Arthur is interested in determining whether the input $x \in L$ and he sends (x, y) to Merlin who responds with a witness z. Arthur does some computations on (x, y, z) following M and decides whether $x \in L$ with high confidence.

A classic example of a problem in AM is that of checking whether a set is large. We keep referring to its AM protocol in this paper.

Proposition 3.2. *Suppose S is a set whose membership can be tested in nondeterministic polynomial time and its size is either m or $2m$. Then the decision problem of testing whether S is of size $2m$ is in AM.*

Proof. The idea of the AM protocol is that if S is large then for a random hash function h there will be an $x \in S$ such that $h(x) = 0$ with high probability.

Suppose that the elements of S are represented as binary strings of length s. Arthur first increases the 'gap' in the size of S by defining a new set $T = S^4$. Now $\#T$ is either m^4 or $16m^4$. Also, the elements of T are binary strings of length $4s$ and view them as a column vector. Arthur then chooses a random 0/1 matrix A of size $\lceil \log 3m^4 \rceil \times 4s$ and sends it to Merlin. Merlin returns a column vector $t \in \{0,1\}^{4s}$ with a membership (in T) proof t'. Arthur accepts iff $t \in T$ and $A \cdot t = 0 \pmod 2$.

To analyse this AM protocol note that for a given $x \in \{0,1\}^{4s} \setminus \{0\}^{4s}$:

$$\mathrm{Prob}_{A \in \{0,1\}^{\lceil \log 3m^4 \rceil \times 4s}} \big[A \cdot x = 0 \ (\mathrm{mod}\ 2) \big] = \frac{1}{2^{\lceil \log 3m^4 \rceil}} \,.$$

Thus by linearity of expectation:

$$E_{A \in \{0,1\}^{\lceil \log 3m^4 \rceil \times 4s}} \Big[\#\big\{ t \in T \mid A \cdot t = 0 \ (\mathrm{mod}\ 2) \big\} \Big] = \frac{\#T}{2^{\lceil \log 3m^4 \rceil}} \,.$$

Now Markov inequalities give us that:

$$\begin{aligned} \#T = 16m^4 &\Rightarrow \mathrm{Prob}_{A \in \{0,1\}^{\lceil \log 3m^4 \rceil \times 4s}} \big[\exists t \in T,\ A \cdot t = 0 \ (\mathrm{mod}\ 2) \big] \geq \frac{5}{8} \,, \\ \#T = m^4 &\Rightarrow \mathrm{Prob}_{A \in \{0,1\}^{\lceil \log 3m^4 \rceil \times 4s}} \big[\exists t \in T,\ A \cdot t = 0 \ (\mathrm{mod}\ 2) \big] \leq \frac{1}{3} \,. \end{aligned}$$

This shows that with high probability Arthur accepts only when set S is large.

Also, note that this AM protocol uses $O(s \log m)$ random bits (for A) and $O(s + |t'|)$ nondeterministic bits (for t and t'). □

If a problem L is in NP$\cap$coNP then intuition suggests that it should not be "hard". Similarly, if a problem L is in NP $\cap$ coAM (or AM $\cap$ coAM) then L is 'unlikely' to be NP-hard. What makes these classes interesting is that there are many problems in NP $\cap$ coAM that are not known to be in P. Such problems are called problems of "intermediate" complexity. To make these notions more precise we need to form a polynomial-time hierarchy.

Let us denote NP by Σ_1 and define $\Sigma_2 = \mathrm{NP}^{\mathrm{NP}}$, where by $\mathrm{NP}^{\mathcal{C}}$ we mean set of languages L such that there is a polynomial time deterministic Turing Machine M using an *oracle* to $\mathcal{C}$ and a positive number c such that:

$$L = \left\{x \mid \ \exists y \in \{0,1\}^{|x|^c},\ M(x,y) \text{ accepts}\right\}.$$

Similarly, $\Sigma_k := \mathrm{NP}^{\Sigma_{k-1}}$. The union of all these Σ's is called the *polynomial-time hierarchy*: $\mathrm{PH} = \cup_{k\geq 1}\Sigma_k$.

It is mostly believed that $\Sigma_1, \Sigma_2, \ldots$ are all distinct complexity classes and hence there is no k such that PH collapses to Σ_k. Coming back to the intermediate complexity classes, it is easy to see that if NP $\cap$ coNP has a NP-hard problem then PH $= \Sigma_1$. Also, if NP $\cap$ coAM (or AM $\cap$ coAM) has a NP-hard problem then it was shown in Boppana *et al.* (1987); Schöning (1988) that PH collapses to the second level Σ_2. The proof goes through by showing that AM $\cap$ coAM is *low for* Σ_2, i.e., $\Sigma_2^{\mathrm{AM}\cap\mathrm{coAM}} = \Sigma_2$ and thus, NP $\subseteq$ AM $\cap$ coAM implies $\Sigma_3 = \Sigma_2^{\mathrm{NP}} \subseteq \Sigma_2^{\mathrm{AM}\cap\mathrm{coAM}} = \Sigma_2$ which eventually results in collapsing PH to Σ_2.

This notion of intermediate complexity can be generalized to *functional problems*. We define FP to be the set of functional problems computable in polynomial time. Now the functional problems in $\mathrm{FP}^{\mathrm{AM}\cap\mathrm{coAM}}$ are of intermediate complexity. If a function $f \in \mathrm{FP}^{\mathrm{AM}\cap\mathrm{coAM}}$ is NP-hard (i.e., NP $\subseteq \mathrm{P}^f$) then the techniques of Schöning (1988) essentially show that PH collapses to Σ_2, an 'unlikely' event. Further, define *functional AM* – denoted by fnAM – to contain functions $f : \{0,1\}^* \to \{0,1\}^*$ such that there is a deterministic polynomial time Turing machine M (that *outputs* a string) and a positive number c such that, for all $x,\ t \in \{0,1\}^*$:

$$(3.3) \qquad f(x) = t \quad \text{iff} \quad \mathrm{Prob}_{y\in\{0,1\}^{|x|^c}}\left[\exists z \in \{0,1\}^{|x|^c}\ M(x,y,z) = t\right] \geq \frac{2}{3}.$$

Remark 3.4. *The above definition says that for "most" of the y 's there is a z such that $M(x,y,z)$ outputs the correct value of $f(x)$. On the other hand, for "most" of the y 's there is no z such that $M(x,y,z)$ outputs an incorrect value.*

Again the techniques of Schöning (1988) essentially show that fnAM is low for Σ_2, i.e., $\Sigma_2^{\mathrm{fnAM}} = \Sigma_2$. Thus, if a function $f \in$ fnAM is NP-hard (i.e., NP $\subseteq \mathrm{P}^f$) then PH collapses to Σ_2. We sketch the proof here for the sake of completeness. Define for all $k \geq 1$, $\Pi_k :=$ co-Σ_k.

PROPOSITION 3.5. $\Sigma_2^{fnAM} = \Sigma_2$.

PROOF. Let a language $L \in \Pi_2^{\mathrm{fnAM}}$. Then, by definition, there is a positive number c and a polynomial time deterministic Turing Machine A using functions from fnAM as *oracles* such that:

$$L = \Big\{x \mid \big(\forall y \in \{0,1\}^{|x|^c}\big)\big(\exists z \in \{0,1\}^{|x|^c}\big)\ \big[A^{\{f_1,\ldots,f_m\}}(x,y,z) \text{ accepts}\big] \\ \text{where, } f_1,\ldots,f_m \in \text{fnAM and } m \leq |x|^c\Big\}. \tag{3.6}$$

Suppose on input x, A queries f_i at strings $w_{i,j} \in \{0,1\}^{|x|^c}$ where i, j are upper-bounded by $|x|^c$. Now from defining (3.3) we have that there is a deterministic polynomial time Turing machine M_i (that *outputs* a string) and a positive number c_i such that:

(3.7)

$$f_i(w_{i,j}) = t_{i,j} \quad \text{iff} \quad \mathrm{Prob}_{y\in\{0,1\}^{|x|^{c_i}}}\big[\exists z \in \{0,1\}^{|x|^{c_i}}\ M_i(w_{i,j},y,z) = t_{i,j}\big] \geq \frac{2}{3}.$$

Now combining (3.7) for various i, j (after probability amplification) and then plugging in (3.6) we get that there is a deterministic polynomial time Turing machine B (that basically simulates M_i 's to compute f_i 's and then runs A to decide L) and a positive number d such that:

$$L = \Bigg\{x \mid \big(\forall y \in \{0,1\}^{|x|^c}\big)\big(\exists z \in \{0,1\}^{|x|^c}\big) \\ \mathrm{Prob}_{u\in\{0,1\}^{|x|^d}}\big[\exists v \in \{0,1\}^{|x|^d},\ B(u,v,x,y,z) \text{ accepts}\big] \geq \frac{2}{3}\Bigg\}$$

$$= \Bigg\{x \mid \big(\forall y \in \{0,1\}^{|x|^c}\big)\ \mathrm{Prob}_{u\in\{0,1\}^{|x|^{d'}}}\Big[\big(\exists z \in \{0,1\}^{|x|^c}\big) \\ \big(\exists v \in \{0,1\}^{|x|^d}\big)\ B'(u,v,x,y,z) \text{ accepts}\Big] \geq \frac{2}{3}\Bigg\}$$

$\big[\because$ By Swapping Lemma 9.14 there is a d' and B' s.t. the above holds$\big]$

$$= \Big\{x \mid \ \big(\forall y \in \{0,1\}^{|x|^c}\big)\big(\forall u_1 \in \{0,1\}^{|x|^e}\big)\big(\exists u_2 \in \{0,1\}^{|x|^e}\big)\big(\exists z \in \{0,1\}^{|x|^c}\big)$$
$$\big(\exists v \in \{0,1\}^{|x|^d}\big)\ \big[B''(u_1, u_2, v, x, y, z) \text{ accepts}\big]\Big\}$$
$$\big[\because e \text{ and } B'' \text{ exists by Lemma 9.14}\big]$$
$$\in \Pi_2\,.$$

Consequently, $\Pi_2^{\mathrm{fnAM}} = \Pi_2$ and hence, $\Sigma_2^{\mathrm{fnAM}} = \Sigma_2$. □

The definitions of ring isomorphism problems are inspired from graph isomorphism (GI) problems that have been open for a long time. But the graph isomorphism problems are not believed to be NP-hard. The AM protocol for graph nonisomorphism was one of the first interactive protocols (see Goldwasser *et al.* 1989) proving that GI $\in$ NP $\cap$ coAM.

The results in this paper mostly *reduce* one problem L to another problem L'. If there is a function $f : \{0,1\}^* \to \{0,1\}^*$ in class $\mathcal{C}$ such that $x \in L$ iff $f(x) \in L'$ then we say that L is *many-one reducible* to L' and denote it by $L \le_m^{\mathcal{C}} L'$.

If a problem L can be solved in class $\mathcal{C}$ by using L' as an oracle then we say that L is *Turing reducible* to L' and denote it by $L \le_T^{\mathcal{C}} L'$.

In the reductions given in this chapter $\mathcal{C}$ is either P or ZPP – the set of languages (functions) that can be decided (computed) in *expected* polynomial time.

4. The complexity of ring isomorphism problem

In this section we prove upper and lower bounds on the complexity of Ring Isomorphism problem. Specifically, we show that RI is in NP $\cap$ coAM and the Graph Isomorphism problem reduces to RI.

4.1. An upper bound. This work has been unable to solve the ring isomorphism problem in polynomial time or even subexponential time. But we show in this section that atleast the problem is unlikely to be NP-hard. Thus, RI becomes a natural example of an intermediate problem which also has a rich algebraic flavor to it.

Theorem 4.1. *RI $\in$ NP $\cap$ coAM.*

Proof. We start with the easier part.

Claim 4.2. *RI* $\in$ *NP*.

Proof (Claim 4.2). Suppose we are given two rings R and R' together with a map $\phi : R \to R'$. Following the remark of Proposition 2.11, we have an algorithm that gives us a description of the rings R, R' over the same additive basis, say,

$$(\mathbb{Z}/m_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m_n\mathbb{Z}) .$$

Thus, we can assume without loss of generality that the rings R, R' are provided as:

$$(R,+) = (\mathbb{Z}/m_1\mathbb{Z})b_1 \oplus \cdots \oplus (\mathbb{Z}/m_n\mathbb{Z})b_n ,$$
$$(R',+) = (\mathbb{Z}/m_1\mathbb{Z})b'_1 \oplus \cdots \oplus (\mathbb{Z}/m_n\mathbb{Z})b'_n .$$

Now ϕ is an isomorphism from $R \to R'$ iff it satisfies the following conditions:

- ϕ *preserves addition*: check whether for all $1 \le i \le n,\ \ m_i \cdot \phi(b_i) = 0$.
- ϕ *preserves multiplication*: check whether for all $1 \le i, j \le n,\ \phi(b_i) \cdot \phi(b_j) = \sum_{k=1}^{n} a_{i,j,k}\phi(b_k)$, where $((a_{i,j,k}))_{i,j,k\in[n]}$ is the same matrix as given in the description of R.
- ϕ *is an invertible map from* $(R,+)$ *to* $(R',+)$: check whether $det(A) \in (\mathbb{Z}/(m_1m_2\ldots m_n)\mathbb{Z})^*$, where A is the $n \times n$ integer matrix describing the map $\phi : R \to R'$.

The first two conditions above imply that ϕ is a homomorphism between the two rings. The third condition ensures that ϕ is bijective. All these three conditions can be checked in polynomial time. □

The next question is whether there are short certificates to prove that two given rings are nonisomorphic, i.e., is RI $\in$ coNP? We are able to tweak the AM protocol for graph nonisomorphism to show that RI is in the randomized version of coNP.

Claim 4.3. *RI* $\in$ *coAM*.

Proof (Claim 4.3). Arthur has two rings R_1, R_2 in basis forms and he wants a *proof* of their non-isomorphism from Merlin. Arthur checks whether $(R_1,+) \cong (R_2,+)$ (see the remark of Proposition 2.11), if not then Arthur already has a proof of non-isomorphism. So assume that $(R_1,+) \cong (R_2,+)$ and now Merlin can provide the descriptions of $(R_1,+),(R_2,+)$ in the form:

$$\begin{aligned}(R_1,+) &= \bigoplus_{i=1}^{n}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})b_i \quad \text{and}\\ (R_2,+) &= \bigoplus_{i=1}^{n}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})c_i, \text{ where } p_i\text{'s are primes and } \alpha_i \in \mathbb{Z}^{\geq 1}\,.\end{aligned}$$

Arthur checks the primality of p_i's and that the above is a basis representation of the rings R_1 and R_2. Let us define sets $C(R_1), C(R_2)$ that we will be using to give an AM protocol for ring non-isomorphism. They will have the nice property that their sizes can be computed *easily* and that $C(R_1) = C(R_2)$ if and only if $R_1 \cong R_2$.

$$\begin{aligned}C(R_1) := \Big\{ &\big\langle ((a_{i,j,k}))_{i,j,k\in[n]}, A_\phi \big\rangle \mid \exists \pi \in Aut(R_1,+) \text{ s.t.}\\ &\text{for all } i,j \in [n],\ \pi(b_i)\cdot\pi(b_j) = \sum_{k=1}^{n} a_{i,j,k}\pi(b_k)\,;\\ &\text{for all } i,j,k \in [n],\ 0 \leq a_{i,j,k} < p_k^{\alpha_k}\,;\\ &A_\phi \text{ is an integer matrix describing some } \phi \in Aut(R_1)\\ &\text{with respect to the additive basis } \big\{\pi(b_i)\big\}_{i=1}^{n} \text{ of } R_1 \Big\}\,.\end{aligned}$$

$C(R_2)$ is defined similarly by replacing the b_i's above by the c_i's and R_1 by R_2. (Note that in the case of graph isomorphism we consider all permutations on the vertices, here we consider all automorphisms of the additive group.)

Observe that:

$$\begin{aligned}\#C(R_1) &= \Big(\text{number of representations } ((a_{i,j,k}))_{i,j,k\in[n]} \text{ of ring } R_1\\ &\qquad \text{over } \bigoplus_{i=1}^{n}\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\Big)\cdot \#Aut(R_1)\\ &= \frac{\#Aut(R_1,+)}{\#Aut(R_1)}\cdot \#Aut(R_1)\\ &= \#Aut(R_1,+)\end{aligned}$$

that can be computed in polynomial time when $(R_1,+)$ is given in terms of basis elements all having prime-power additive orders (see Proposition 2.13). Thus, Arthur can compute $s := \#C(R_1) = \#C(R_2)$.

Define $C(R_1, R_2) := C(R_1) \cup C(R_2)$. Note that:

$$\begin{aligned} R_1 \cong R_2 &\Rightarrow C(R_1) = C(R_2) \\ &\Rightarrow \#C(R_1, R_2) = \#C(R_1) = s\,. \\ R_1 \not\cong R_2 &\Rightarrow C(R_1) \cap C(R_2) = \emptyset \\ &\Rightarrow \#C(R_1, R_2) = \#C(R_1) + \#C(R_2) = 2s\,. \end{aligned}$$

Thus, the size of the set $C(R_1, R_2)$ has a gap factor of 2 between the cases of $R_1 \cong R_2$ and $R_1 \not\cong R_2$, which can be distinguished by the AM protocol of Proposition 3.2.

Note that this AM protocol for ring nonisomorphism requires:

$$O\big((\log^4 \#R_1) \cdot (\log s)\big) = O(\log^7 \#R_1)$$

random bits, and $O(\log^4 \#R_1)$ nondeterministic bits. □

The two claims show that RI is in NP $\cap$ coAM. □

This shows that the ring isomorphism problem cannot be NP-hard (unless polynomial hierarchy collapses to Σ_2, Schöning 1988).

4.2. A lower bound: reduction from graph isomorphism. The proofs above were all similar in spirit to those for graph isomorphism which hints a connection to graph isomorphism. Indeed, we can lower bound the complexity of RI by graph isomorphism (GI). The reduction gives a way to construct a local commutative ring out of a given graph.

Theorem 4.4. ***GI*** $\le_m^P$ ***RI***.

Proof. The proof involves constructing a commutative local ring that captures the "adjacency" of a given graph. We associate variables to each vertex (v-variable) and pair of vertices (a-variable). The additive order of a variable encodes whether the variable corresponds to a vertex or an edge or a non-edge of the graph. The product of two vertex-variables is defined to be an a-variable while the other type of products are defined to be zero.

Given a graph G with n vertices and m edges. Choose an odd prime p and let $\ell := \binom{n}{2}$. Let $\{a_k\}_k$ be a set of ℓ variables indexed by $k \in \{(i,j) \mid 1 \le i < j \le n\}$. Define the following *commutative* ring:

$$R(G) := (\mathbb{Z}/p^3\mathbb{Z})[v_1, \ldots, v_n, a_1, \ldots, a_\ell]/\mathcal{I}\,,$$

where ideal $\mathcal{I}$ has the following relations:

1. for all $1 \leq i \leq n$: $v_i^2 = 0$,
2. for all $1 \leq i < j \leq n$: $v_j v_i = v_i v_j = a_e$ where, $e = (i, j)$,
3. for all i, j: $a_j v_i = v_i a_j = 0,\ a_i a_j = 0$,
4. for all $1 \leq i < j \leq n$: if $e = (i, j) \in E(G)$ then $pa_e = 0$ else $p^2 a_e = 0$.

The v_i's represent the n vertices and have an additive order of p^3. The a_i's with additive order p are for the m edges. Finally, the a_i's with additive order p^2 represent the $(\ell - m)$ non-edges.

The additive structure of the ring is:

$$\big(R(G), +\big) = (\mathbb{Z}/p^3\mathbb{Z}) \oplus \bigoplus_{i=1}^{n} (\mathbb{Z}/p^3\mathbb{Z}) v_i \oplus \bigoplus_{e \in E(G)} (\mathbb{Z}/p\mathbb{Z}) a_e \oplus \bigoplus_{e \notin E(G)} (\mathbb{Z}/p^2\mathbb{Z}) a_e \,.$$

Multiplication satisfies the associative law simply because the product of any three *variables* (in any order) is zero.

Observe that if $G \cong G'$ then any graph isomorphism ϕ induces a natural isomorphism between rings $R(G)$ and $R(G')$. So we only have to prove the converse:

CLAIM 4.5. *For any two undirected graphs (having no self-loops) G and G', if $R(G) \cong R(G')$ then $G \cong G'$.*

PROOF (Claim 4.5). Suppose ϕ is an isomorphism from $R(G) \to R(G')$. Let

$$\phi(v_1) = c_{1,0} + c_{1,1} v_1' + \cdots + c_{1,n} v_n' + (\text{linear combination of } a_i' s)\,, \tag{4.6}$$

where all coefficients are in $\mathbb{Z}/p^3\mathbb{Z}$.

Since, $\phi(v_1)^2 = 0$ we get:

$$c_{1,0}^2 + (2c_{1,0}c_{1,1}) v_1' + \cdots + (2c_{1,0}c_{1,n}) v_n' + (\text{linear combination of } a_i' s) = 0\,.$$

As $1, v_i' s$ and $a_j' s$ form an additive basis of $R(G')$, we conclude:

$$c_{1,0}^2 = 2c_{1,0}c_{1,1} = \cdots = 2c_{1,0}c_{1,n} = 0 \ (\text{mod } p^3)\,.$$

Since p is an odd prime, if $c_{1,0} \neq 0(\text{mod } p^3)$ then $p | c_{1,0}, c_{1,1}, \ldots, c_{1,n}$. But then by (4.6), $p^2 \phi(v_1) = 0$ which is a contradiction to the fact that ϕ is an isomorphism. Thus, $c_{1,0} = 0(\text{mod } p^3)$. Now at least one of the $c_{1,i}$'s has to be a unit (i.e., coprime to p) otherwise again by (4.6), $p^2\phi(v_1) = 0$. Say, c_{1,i_0} is a unit. From the equation:

$$0 = \phi(v_1)^2 = \sum_{1\le i<j\le n} (2c_{1,i}c_{1,j})v_i'v_j' \tag{4.7}$$

it follows that if $(i_0, j) \in E(G)$, for some $j \neq i_0$, then $p|c_{1,j}$ else $p^2|c_{1,j}$. Thus, we have shown that *exactly* one of the $c_{1,1}, \ldots, c_{1,n}$ is a unit. So we can define a map $\pi : [n] \to [n]$ with $\pi(1) = i_0$ and satisfying the following condition for all $1 \le i \le n$:

$$\phi(v_i) = c_{i,\pi(i)}v'_{\pi(i)} + p.\sum_{\substack{j=1\\ j\neq\pi(i)}}^{n} d_{i,j}v_j' + (\text{linear combination of } a_k's)\,, \tag{4.8}$$

where all coefficients are in $\mathbb{Z}/p^3\mathbb{Z}$ and $c_{i,\pi(i)}$ is a unit.

Now observe that $\phi(v_i)^2 = 0$ and $\phi(v_j)^2 = 0$ means that (simply by squaring (4.8)):

$$p.\sum_{\substack{k=1\\ k\neq\pi(i)}}^{n} d_{i,k}v_k'v'_{\pi(i)} = 0$$

and

$$p.\sum_{\substack{k=1\\ k\neq\pi(j)}}^{n} d_{j,k}v_k'v'_{\pi(j)} = 0\,. \tag{4.9}$$

Thus, if $\pi(i) = \pi(j)$ then calculation shows (using (4.8) and (4.9)) that $\phi(v_i)\phi(v_j) = 0$ implying that $\phi(v_iv_j) = 0$ which forces $i = j$. Hence, π is a permutation on $[n]$.

We are now almost done, we just have to show that π is indeed an isomorphism from the graph $G \to G'$.

Suppose $e = (i, j) \in E(G)$. Thus, (using (4.8))

$$\phi(a_e) = \phi(v_iv_j) = (c_{i,\pi(i)}c_{j,\pi(j)})v'_{\pi(i)}v'_{\pi(j)} + p\cdot(\text{linear combination of } a_k's)\,.$$

Since, $p\cdot\phi(a_e) = 0$ and $c_{i,\pi(i)}c_{j,\pi(j)}$ is a unit we get:

$$p\cdot v'_{\pi(i)}v'_{\pi(j)} = 0\,.$$

Whence, we conclude that $v'_{\pi(i)}v'_{\pi(j)}$ is of additive order p implying, by the definition of $R(G')$, that $(\pi(i), \pi(j)) \in E(G')$.

By symmetry this shows that π is an isomorphism from $G \to G'$. □

The theorem follows from the claim. □

Note that even if graph G is rigid (i.e., G has only trivial automorphism) the ring $R(G)$ has lots of nontrivial automorphisms, for example, $\phi : x_i \mapsto x_i + x_1 x_2$. Thus, unfortunately, this reduction does not reduce the problem of testing rigidity of graphs to testing rigidity of rings.

4.3. Table representation: is it any easier?. One can also consider a different, exponentially larger, representation for rings: when the rings are given in terms of the addition and multiplication tables of all its elements. We do not know if the ring isomorphism problem even under this representation can be solved in time polynomial in the size of the representation. However, there is a feeling that this version of ring isomorphism should be easier as there is a simple subexponential algorithm: Suppose rings R_1, R_2 are of size n. Then the additive group of R_1 will have $O(\log n)$ generators and there are $n^{O(\log n)}$ ways to map these generators into R_2. Thus, a brute-force search over all these maps yields a $n^{O(\log n)}$ time algorithm for ring isomorphism.

Here we give another theoretical evidence that the problem is easy by showing that it is "almost" in NP $\cap$ coNP.

Let us give this problem a name:

$$\mathrm{RI}_{TF} := \left\{(R_1, R_2) \mid R_1, R_2 \text{ are given in terms of tables, } R_1 \cong R_2\right\}.$$

It is easy to see that $\mathrm{RI}_{TF} \in$NP. The nontrivial part is to show:

Theorem 4.10. *There exists an NP-machine that decides all but $2^{\log^{11} n}$ instances of $\overline{RI}_{TF}$ of length n and is always correct when the input rings are nonisomorphic.*

Proof. The proof is basically the one given in Arvind & Torán (2004) applied to the case of rings.

We showed in Claim 4.3 that $\overline{\mathrm{RI}}_{TF} \in \mathrm{AM}(\log^7 n)$, where the parameter bounds the number of random bits used by Arthur. We interpret this result to mean that there is an advice-taking NP machine $M(\cdot,\cdot)$ for $\overline{\mathrm{RI}}_{TF}$ such that:

$$\forall \text{ input } x \in \{0,1\}^n,\ \mathrm{Prob}_{y \in \{0,1\}^{\log^7 n}}\left[M(x,y) \text{ is correct}\right] \geq \frac{2}{3}.$$

Notice that since a ring is completely defined once we specify the multiplication on the additive generators, we have that the number of binary strings of length n that define a ring, in table form, is no more than $2^{\log^4 n}$. Thus, using probability amplification we modify M to get an advice-taking NP machine M' for $\overline{\mathrm{RI}}_{TF}$ such that:

$$\mathrm{Prob}_{y\in\{0,1\}^{\log^{11} n}}\big[\forall x \in \{0,1\}^n,\ M'(x,y) \text{ is correct}\big] \geq \frac{2}{3}\,.$$

Since we are using only a "small" number of random bits we can apply techniques of Goldreich & Wigderson (2002) to get an NP-machine for $\overline{\mathrm{RI}}_{TF}$ that fails for at most $2^{\log^{11} n}$ inputs of size n and is always correct when the input rings are nonisomorphic. □

5. The complexity of counting ring automorphisms

This section will explore the complexity of the problem of counting ring automorphisms. We will show that this problem is unlikely to be NP-hard but both graph isomorphism and integer factoring reduce to it.

5.1. An upper bound. We will show that given a finite ring R there is an AM protocol in which Merlin sends a number ℓ and convinces Arthur that $\#Aut(R) = \ell$. The ideas in the proof are basically from Babai & Szemerédi (1984).

THEOREM 5.1. *$\#RA \in FP^{AM\cap coAM}$.*

PROOF. Let R be a finite ring given in its basis form. We will first show how Merlin can convince Arthur that $\#Aut(R) \geq k$. Recall that in (2.4) we defined this problem as cRA.

CLAIM 5.2. *$cRA \in AM$.*

PROOF (Claim 5.2). Merlin can give Sylow subgroups $S_{p_1}, \dots, S_{p_m}$ of $Aut(R)$, in terms of generators, to Arthur such that $p_1, \dots, p_m$ are distinct primes and the product $|S_{p_1}|.\cdots.|S_{p_m}| \geq k$. Arthur now has to verify whether for a given Sylow subgroup S_p, $|S_p| = p^t$ or not. So Merlin can further provide the composition series of S_p:

$$S_p = G_t > G_{t-1} > \cdots > G_1 > G_0 = \{1\}\,.$$

Suppose, by induction, that Arthur is convinced about $|G_i| = p^i$. Then to prove $|G_{i+1}| = p^{i+1}$, Merlin will provide $x_{i+1} \in G_{i+1}$ to Arthur with the claim that $x_{i+1} \notin G_i$ but $x_{i+1}^p \in G_i$. Latter can be verified easily by Arthur as Merlin can give the way to produce x_{i+1}^p from the generators of G_i. Finally, the only nontrivial thing left for Arthur to verify is whether $x_{i+1} \notin G_i$, which can be verified by a standard AM protocol (Proposition 3.2) as there is a gap in the size of the set $X :=$ (group generated by x_{i+1} and G_i):

$$\begin{aligned} x_{i+1} \notin G_i &\Rightarrow \#X = p^{i+1}\,, \\ x_{i+1} \in G_i &\Rightarrow \#X = p^{i}\,. \end{aligned}$$

To avoid too many rounds, Merlin first provides $x_0 = 1, x_1, \ldots, x_t \in Aut(R)$ and the proof of: for all $1 \le i \le t$, $x_i^p \in G_{i-1} :=$ (group generated by $x_0, \ldots, x_{i-1}$) to Arthur and then provides the proof of: for all $1 \le i \le t$, $x_i \notin G_{i-1}$ in the second round for Arthur to verify. □

Now we give the AM protocol that convinces Arthur of $\#Aut(R) \le k$.

Claim 5.3. *cRA* $\in$ *coAM*.

Proof (Claim 5.3). Arthur has a finite ring R and he wants a proof of $\#Aut(R) \le k$. As in the proof of Claim 4.3, we can assume that R is given in terms of generators having prime-power additive orders. For concreteness let us assume:

$$(R, +) = \bigoplus_{i=1}^{n} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) b_i\,.$$

Merlin sends Arthur a number $\ell \le k$ as a candidate value for $\#Aut(R)$ and also provides some Sylow subgroups, the product of their sizes being equal to ℓ, with the AM-proofs for their sizes (as used in Claim 5.2). Let

$$X := \left\{ \langle ((a_{i,j,k}))_{i,j,k \in [n]} \rangle \mid \exists \pi \in Aut(R,+) \text{ s.t. } \pi(b_i) \cdot \pi(b_j) = \sum_{k=1}^{n} a_{i,j,k} \pi(b_k)\,; \right.$$
$$\left. \text{for all } 1 \le i,j,k \le n,\ 0 \le a_{i,j,k} < p_k^{\alpha_k} \right\}.$$

Observe that $\#X = \frac{\#Aut(R,+)}{\#Aut(R)}$ and $\#Aut(R,+)$ can be computed in polynomial time when $(R,+)$ is given in terms of generators having prime-power additive orders (see Proposition 2.13). Thus, Arthur computes $s := \#Aut(R,+)$. Arthur is already convinced that $\ell | \#Aut(R)$ and he now wants to verify whether $\#Aut(R) \le \ell$. A standard AM protocol (see Proposition 3.2) now follows by utilizing the gap in the size of X in the two cases:

$$\begin{aligned} \#Aut(R) \le \ell &\Rightarrow \#X \ge \frac{s}{\ell}\,. \\ \#Aut(R) > \ell &\Rightarrow \#Aut(R) \ge 2\ell \quad [\because \#Aut(R) \text{ has a subgroup of size } \ell] \\ &\Rightarrow \#X \le \frac{s}{2\ell}\,. \end{aligned}$$ □

The claims above show that $\#\mathrm{RA} \in \mathrm{FP}^{\mathrm{cRA}} \subseteq \mathrm{FP}^{\mathrm{AM}\cap\mathrm{coAM}}$. □

Note that the AM protocols that we give for #RA not only count the number of automorphisms but give a lot more information about the automorphism group. In fact, these AM protocols compute the full automorphism group of a ring R in terms of the generators of the Sylow subgroups of $Aut(R)$. Let us denote the functional problem of *computing the group of automorphisms* of a ring given in basis form by GroupRA.

Corollary 5.4. *Function GroupRA $\in$ fnAM and hence is low for Σ_2.*

Proof. Let f be the function, corresponding to GroupRA, that maps a ring R (given in basis form) to the tuple $(\#Aut(R), Aut(R))$. Since cRA is in both AM and coAM there are deterministic polynomial time Turing Machines A and B, and positive constants c, d such that:

$$\begin{aligned} \#Aut(R) \le k \quad \text{iff} \quad & \mathrm{Prob}_{y\in\{0,1\}^{\log^c \#R}}\Big[\big(\exists z \in \{0,1\}^{\log^c \#R}\big)\ A(R,k,y,z) \text{ accepts}\Big] \\ & \ge \left(1 - \frac{1}{2^{\log^d \#R}}\right), \\ \#Aut(R) \ge k \quad \text{iff} \quad & \mathrm{Prob}_{y\in\{0,1\}^{\log^c \#R}}\Big[\big(\exists z \in \{0,1\}^{\log^c \#R}\big)\ B(R,k,y,z) \text{ accepts}\Big] \\ (5.5) \qquad & \ge \left(1 - \frac{1}{2^{\log^d \#R}}\right). \end{aligned}$$

The parameter d above will be chosen large enough so that all the subsequent arguments go through. To show that $f \in$ fnAM we plan to run A and B in parallel. We can modify A slightly to A' by requiring that $A(R,k,y,z)$ outputs (ℓ, G) where, ℓ is the number and G is the group, given by the generators of the (intended) Sylow subgroups, as occurred in the proof of the Claim 5.3. It is easy to see that:

$$\begin{aligned} & f(R) = (m,H) \\ & \quad \Rightarrow \mathrm{Prob}_{y\in\{0,1\}^{2\log^c \#R}}\Big[\big(\exists \ell' z z' \in \{0,1\}^{3\log^c \#R}\big),\ \text{both } A'(R,\ell',y,z) \\ (5.6) \qquad & \quad\quad \text{and } B(R,\ell',y,z') \text{ accept and } A'(R,\ell',y,z) = (m,H)\Big] \ge \frac{3}{4}\,. \end{aligned}$$

The above holds because Merlin can simply send ℓ' as equal to $\#G$ and a part of the string z and z' having the group $Aut(R)$ in terms of the generators of Sylow subgroups (see the proof of Claim 5.3). Then (5.5) give us the probability lower bound of $\frac{3}{4}$. Also, the output of $A'(R, \ell', y, z)$ for such ℓ', z will trivially be (m, H).

To show the converse assume that there is a number m and a group H such that:

$$\begin{aligned}&\mathrm{Prob}_{y \in \{0,1\}^{2\log^c \#R}}\Big[\big(\exists \ell' z z' \in \{0,1\}^{3\log^c \#R}\big), \text{ both } A'(R, \ell', y, z) \\ &\qquad \text{and } B(R, \ell', y, z') \text{ accept and } A'(R, \ell', y, z) = (m, H)\Big] \geq \frac{3}{4}\,. \end{aligned} \tag{5.7}$$

Now if $(m, H) \neq (\#Aut(R), Aut(R))$ then the way A' outputs, it is clear that Merlin tried to "fool" Arthur and so by the (5.5) we get that for some positive d':

$$\begin{aligned}&\mathrm{Prob}_{y \in \{0,1\}^{2\log^c \#R}}\Big[\big(\exists \ell' z z' \in \{0,1\}^{3\log^c \#R}\big), \text{both } A'(R, \ell', y, z) \text{ and} \\ &\quad B(R, \ell', y, z') \text{ accept } \mid A'(R, \ell', y, z) \neq \big(\#Aut(R), Aut(R)\big)\Big] \leq \frac{1}{2^{\log^{d'} \#R}}\,.\end{aligned}$$

which together with the large probability lower bound of (5.7) means that: $(m, H) = (\#Aut(R), Aut(R))$. Thus,

$$\begin{aligned}&\mathrm{Prob}_{y \in \{0,1\}^{2\log^c \#R}}\Big[\big(\exists \ell' z z' \in \{0,1\}^{3\log^c \#R}\big), \text{ both } A'(R, \ell', y, z) \\ &\qquad \text{and } B(R, \ell', y, z') \text{ accept and } A'(R, \ell', y, z) = (m, H)\Big] \geq \frac{3}{4} \\ &\Rightarrow \quad f(R) = (m, H).\end{aligned} \tag{5.8}$$

Recall (3.3) for the definition of fnAM, clearly, (5.6) and (5.8) tell us that: $f \in$ fnAM. □

5.2. A lower bound: reduction from graph isomorphism and integer factoring. This section shows that #RA is a fairly interesting intermediate problem as two well known problems – one of graphs and another of integers – reduce to it.

In the case of graphs it is easy to show that graph isomorphism (or counting graph isomorphisms) reduces to counting graph automorphisms. The same result continues to hold for rings with a slightly more involved proof. In the case of graphs we take disjoint union of graphs to construct a new graph, here we take *direct product* of rings to construct a new ring. It turns out that the number of automorphisms of this new ring can be used to find out whether the original rings were isomorphic or not.

Lemma 5.9. $\#RI \equiv_T^P \#RA$.

Proof. Suppose we are given a ring R. Clearly we can compute $\#Aut(R)$ by giving (R, R) as input to the oracle of #RI.

Conversely, let R_1, R_2 be the two rings given in basis form. Let us assume the following about their decomposability into *distinct* local rings $S_1, \ldots, S_k$:

$$R_1 \cong S_1 \times \cdots \times S_1 \times \cdots \times S_k \times \cdots \times S_k\,,$$

where, for all $1 \leq i \leq k$, indecomposable ring S_i occurs $a_i \geq 0$ times and $\#Aut(S_i) = m_i$.

$$R_2 \cong S_1 \times \cdots \times S_1 \times \cdots \times S_k \times \cdots \times S_k\,,$$

where, for all $1 \leq i \leq k$, indecomposable ring S_i occurs $b_i \geq 0$ times.

The following claim relates the (non)isomorphism of the rings to counting ring automorphisms:

Claim 5.10. $R_1 \ncong R_2 \Rightarrow \#Aut(R_1 \times R_1) \cdot \#Aut(R_2 \times R_2) > (\#Aut(R_1 \times R_2))^2$.

Proof (Claim 5.10). Due to the uniqueness of decomposition of a ring into indecomposable rings (see Proposition 2.15):

$$\begin{aligned}\#Aut(R_1 \times R_2) &= \#Aut(\overbrace{S_1 \times \cdots \times S_1}^{a_1+b_1}) \cdots \#Aut(\overbrace{S_k \times \cdots \times S_k}^{a_k+b_k})\\ &= (a_1+b_1)!m_1^{a_1+b_1} \cdots (a_k+b_k)!m_k^{a_k+b_k}\,,\end{aligned}$$

Similarly,

$$\begin{aligned}\#Aut(R_1 \times R_1) &= \#Aut(\overbrace{S_1 \times \cdots \times S_1}^{2a_1}) \cdots \#Aut(\overbrace{S_k \times \cdots \times S_k}^{2a_k})\\ &= (2a_1)!m_1^{2a_1} \cdots (2a_k)!m_k^{2a_k}\,,\end{aligned}$$

$$\begin{aligned}\#Aut(R_2 \times R_2) &= \#Aut(\overbrace{S_1 \times \cdots \times S_1}^{2b_1}) \cdots \#Aut(\overbrace{S_k \times \cdots \times S_k}^{2b_k})\\ &= (2b_1)!m_1^{2b_1} \cdots (2b_k)!m_k^{2b_k}\,.\end{aligned}$$

Notice that $\binom{2a_i+2b_i}{a_i+b_i} \geq \binom{2a_i+2b_i}{2a_i}$ which implies $(2a_i)! \cdot (2b_i)! \geq (a_i+b_i)!^2$. This clearly shows:

$$\#Aut(R_1 \times R_1) \cdot \#Aut(R_2 \times R_2) \geq \big(\#Aut(R_1 \times R_2)\big)^2\,.$$

Now since $R_1 \ncong R_2$, there exists an $i_0 \in [k]$ such that $a_{i_0} \neq b_{i_0}$ in which case $(2a_{i_0})! \cdot (2b_{i_0})! \gneq (a_{i_0} + b_{i_0})!^2$. Thus,

$$\#Aut(R_1 \times R_1) \cdot \#Aut(R_2 \times R_2) > (\#Aut(R_1 \times R_2))^2. \qquad \square$$

$$\square$$

As a corollary of this we get:

Theorem 5.11. *Graph Isomorphism* $\leq_T^P$ *#RA.*

Proof. Immediate from Theorem 4.4 and Lemma 5.9. □

Another interesting open problem that reduces to #RA is integer factorization (IF).

Theorem 5.12. *IF* $\leq_T^{ZPP}$ *#RA.*

Proof. Let n be the *odd* integer to be factored. Consider the ring

$$R := (\mathbb{Z}/n\mathbb{Z})[x]/(x^2)$$

We will show that $\#Aut(R) = \varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$ (φ is called the Euler's Totient function). The theorem is then immediate as n can be factored in expected polynomial time if we are given $\varphi(n)$, see Miller (1976).

Suppose $\psi \in Aut(R)$ and let $\psi(x) = ax + b$, for some $a, b \in \mathbb{Z}/n\mathbb{Z}$. Since ψ is an automorphism; a, b should satisfy the following two conditions:

$$(ax + b)^2 = 0 \text{ in } R \Rightarrow ab = b^2 = 0 \pmod{n}, \quad \text{and}$$
$$a \in (\mathbb{Z}/n\mathbb{Z})^*.$$

These two conditions force $b = 0$ and any $a \in (\mathbb{Z}/n\mathbb{Z})^*$ will work. Thus, $\#Aut(R) = |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$. □

6. The complexity of finding a ring isomorphism

We have seen by now that ring isomorphism and its counting version are both of intermediate complexity and some well known problems – integer factoring and graph isomorphism – reduce to them. Another interesting variant of RI is its search version – FRI – *finding* an isomorphism between two rings given in basis form. First question that arises here is whether we can find a ring isomorphism given oracles to RI or #RI. This is still open but in this section we show that FRI seems to have a complexity similar to that of RI and #RI.

6.1. An upper bound. FRI is unlikely to be NP hard as we show that it reduces to the problem of computing the automorphism group of a ring – GroupRA. The idea is that if we want to find an isomorphism from a ring R to R' then we consider the ring $S = R \times R'$ and compute the generator set T of $Aut(S)$. Now if $R \cong R'$ then there will be a generator $\phi \in T$ that sends some elements of R to those of R'. We construct an isomorphism from $R \to R'$ using this automorphism ϕ of $R \times R'$.

Theorem 6.1. *FRI* $\in FP^{GroupRA} \subseteq fnAM$.

Proof. Let R, R' be the two isomorphic rings given in basis form. Let their decomposition into indecomposable components be:

$$R = R_1 \times \cdots \times R_s\,,$$
$$R' = R'_1 \times \cdots \times R'_s\,,$$

Suppose an oracle to GroupRA queried on $S := R \times R'$ gives the group $Aut(S)$ in terms of a generator set T. For concreteness, let us fix an additive basis of S: $\{b_1, \ldots, b_n, b'_1, \ldots, b'_n\}$ where $\{b_1, \ldots, b_n\}$ are the basis elements of R and $\{b'_1, \ldots, b'_n\}$ are those of R'. Furthermore, as S is a direct product of R and R' we have: for all $i, j \in [n]$, $b_i \cdot b'_j = b'_i \cdot b_j = 0$. If $R \cong R'$ then there has to be an element $\phi \in T$ that maps some basis elements of R outside R. Fix such an automorphism ϕ. For $i \in [n]$, let:

$$\phi(b_i) = \sum_{j=1}^{n} a_{i,j} b_j + \sum_{j=1}^{n} a'_{i,j} b'_j\,,$$

where $a_{i,j}$'s and $a'_{i,j}$'s are integers modulo the characteristic of S, say N.

Now using linear algebra (over $\mathbb{Z}/N\mathbb{Z}$) we can compute an additive basis of the following subring of R:

$$K := \{r \in R \mid \phi(r) \in R\}\,.$$

Note that K is a (proper) subring of R simply because ϕ is a ring homomorphism. Now since ϕ is an automorphism and the decomposition of a ring into indecomposable rings is unique (see Lemma 9.4 for details) we get that ϕ applied on S permutes $R_1, \ldots, R_s$, $R'_1, \ldots, R'_s$ up to isomorphism. This means that there are $\{i_1, \ldots, i_t\} \subsetneq [s]$ such that:

$$K = R_{i_1} \times \cdots \times R_{i_t}\,.$$

Again by linear algebra we can compute the 'other' component ring:

$$K^{\perp} := \{r \in R \mid K \cdot r = r \cdot K = 0\}\,,$$

which can be shown to satisfy:

$$R = K \times K^{\perp}$$

Now what is the action of ϕ on these? Observe that $\phi(K) \subseteq R$ while $\phi(K^{\perp}) \subseteq R'$. To get a decomposition of R' too, define $L := \phi(K^{\perp})$ and compute:

$$L^{\perp} := \{r \in R' \mid L \cdot r = r \cdot L = 0\}\,,$$

which can again be shown to satisfy:

$$R' = L \times L^{\perp}$$

(as ϕ is an isomorphism from $K^{\perp} \to L$ and $R \cong R'$).

Now recursively find an isomorphism ψ from K to $L^{\perp}$ using GroupRA as oracle. ϕ and ψ together give us an isomorphism from R to R'.

Thus, FRI $\in$ FP$^{\text{GroupRA}}$. □

6.2. A lower bound: reduction from integer factoring. It turns out that solving **FRI** would mean solving integer factoring (**IF**).

THEOREM 6.2. *IF* $\leq_T^{ZPP}$ *FRI.*

PROOF. Suppose n is an odd number to be factored and it is not a prime power. Pick a random $a \in (\mathbb{Z}/n\mathbb{Z})^*$ and define the rings:

$$R_1 := (\mathbb{Z}/n\mathbb{Z})[x]/(x^2 - a^2) \qquad \text{and} \qquad R_2 := (\mathbb{Z}/n\mathbb{Z})[x]/(x^2 - 1)\,.$$

Query the oracle of FRI on (R_1, R_2) to get an isomorphism $\phi : R_1 \to R_2$. Let $\phi(x) = bx + c,\ b, c \in \mathbb{Z}/n\mathbb{Z}$.

Firstly, observe that if b is a zero divisor i.e., there is a $b' \in (\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$ with $bb' = 0$ then $\phi(b'x - b'c) = b'(bx + c) - b'c = 0$ in R_2. As ϕ is an isomorphism this means that $(b'x - b'c) = 0$ in R_1 implying that $b' = 0$ in $\mathbb{Z}/n\mathbb{Z}$ which is a contradiction. Thus, b should be in $(\mathbb{Z}/n\mathbb{Z})^*$.

Secondly, $\phi(x^2 - a^2)$ should be zero in R_2 which means that:

$$\begin{aligned} a^2 = \phi(x)^2 = (bx + c)^2 \ (\text{mod } n, x^2 - 1) \\ \Rightarrow 2bc = 0 (\text{mod } n) \text{ and } b^2 + c^2 - a^2 = 0 (\text{mod } n) \\ \Rightarrow c = 0 (\text{mod } n) \text{ and } b^2 = a^2 (\text{mod } n) \end{aligned}$$

This means that b is a square-root of a^2 modulo n. It is easily seen that when n has two or more prime factors then every square in $(\mathbb{Z}/n\mathbb{Z})^*$ has 4 or more square-roots. Thus,

$$\mathrm{Prob}_{a\in(\mathbb{Z}/n\mathbb{Z})^*}\Big[b \neq \pm a (\mathrm{mod}\ n) \mid b = \sqrt{a^2}(\mathrm{mod}\ n)\Big] \geq \frac{1}{2}\,.$$

Now once we have a $b \neq \pm a(\mathrm{mod}\ n)$ such that $b^2 = a^2(\mathrm{mod}\ n)$ we can factor n by using the standard trick of computing $gcd(b-a,n)$.

Thus, we can factor n in expected polynomial time given an oracle to FRI. □

This reduction from integer factoring shows an interesting aspect of RI. If we modify RI to $\mathrm{RI}_{\mathrm{boundedIso}}$ – decision problem of checking whether there is an isomorphism $\phi : R_1 \to R_2$ such that the corresponding matrix A, which transforms the basis of $(R_1,+)$ to that of $(R_2,+)$, has elements smaller than a given size bound – then it turns out that $\mathrm{RI}_{\mathrm{boundedIso}}$ is NP-complete.

$$\begin{aligned}\mathrm{RI}_{\mathrm{boundedIso}} := \Big\{ & \big(R_1, R_2, ((b_{i,j}))_{n\times n}\big) \mid R_1, R_2 \text{ are rings given in basis form,}\\ & \text{having additive dimension } n \text{ and there is an integer matrix } A,\\ & \text{such that } \forall i,j\ 0 \leq A_{i,j} \leq b_{i,j},\ \text{ that defines an isomorphism.}\Big\}\end{aligned}$$

THEOREM 6.3. *$RI_{boundedIso}$ is NP-complete.*

PROOF. Clearly, $\mathrm{RI}_{\mathrm{boundedIso}}$ is in NP by Claim 4.2.

Suppose we are given $R_1 := (\mathbb{Z}/n\mathbb{Z})[x]/(x^2-a^2)$, $R_2 := (\mathbb{Z}/n\mathbb{Z})[x]/(x^2-1)$, $\beta \in \mathbb{Z}$ and we want to find out whether there is an isomorphism $\phi(x) = bx$ s.t. $0 \leq b \leq \beta$. Now as in the proof of Theorem 6.2, $b^2 \equiv a^2(\mathrm{mod}\ n)$. Thus, the question at hand is equivalent to asking whether the quadratic equation (in y): $y^2 \equiv a^2(\mathrm{mod}\ n)$ has a solution $0 \leq y \leq \beta$, and this is an NP-complete problem by Manders & Adleman (1976). □

7. The complexity of deciding ring automorphism

This section studies the problem of checking whether a given ring is *rigid* (i.e., has no nontrivial automorphism). We will show that RA can be decided in deterministic polynomial time but as the next section shows finding a nontrivial automorphism (FRA) is as hard as integer factoring. Thus, there appears to be a difference in the complexity of decision, search and counting versions of ring automorphism problems. Note the contrast that we (currently) have with the complexity of the corresponding versions for graph automorphism problems, for instance GA is not known to be in P.

THEOREM 7.1. *RA* $\in$ *P*.

We first derive a classification of finite rigid rings and then use that classification to devise an efficient algorithm for RA.

7.1. A classification of finite rigid rings. In this subsection, we shall show that those finite rings which do not have nontrivial automorphisms (rigid rings) have a nice mathematical description which will later be used to test rigidity in polynomial time.

THEOREM 7.2. *Let R be any finite ring with identity. R can be expressed as the direct sum of two rings:*

$$R = R_{2pow} \times R_{odd}\,,$$

where, R_{2pow} is a power-of-2 sized ring while R_{odd} is an odd-sized ring. Then R is rigid if and only if the following conditions hold:

(i) R_{2pow} is of the form:

$$\begin{array}{l} \mathbb{Z}/2^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/2^{\alpha_n}\mathbb{Z} \\ \text{or} \\ (\mathbb{Z}/2\mathbb{Z})[x]/(x^2) \times \mathbb{Z}/2^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/2^{\alpha_n}\mathbb{Z} \\ \text{where, } 1 \le \alpha_1 < \alpha_2 < \cdots < \alpha_n\,. \end{array}$$

(ii) R_{odd} is of the form:

$$\begin{array}{l} \times_i \times_j (\mathbb{Z}/p_i^{\alpha_{i,j}}\mathbb{Z}) \\ \qquad \text{where } p_i\text{'s are distinct odd primes and } 1 \le \alpha_{i,1} < \alpha_{i,2} < \cdots\,. \end{array}$$

PROOF. It is easy to verify the following claim:

CLAIM 7.3. *A ring R is rigid if and only if each one of its indecomposable component rings is rigid and no two of these indecomposable components are isomorphic.*

This means that any arbitary rigid ring is just a direct sum of a set of non-isomorphic indecomposable rigid rings. Thus, to get a classification of finite rigid rings, it is sufficient to get a classification of finite indecomposable rigid rings. In the rest of this proof we give such a characterization of indecomposable rigid rings.

Let R be a ring given in basis form. Let us first dispose off the case when R is non-commutative.

Claim 7.4. *If R is a non-commutative ring then it has a nontrivial automorphism.*

Proof (Claim 7.4). It can be shown (Lenstra 2004) that if the *units* in a ring R commute with the whole of R then R is generated by its units, and consequently R will be commutative. Thus, if R is a non-commutative ring then there is a *unit* $r \in R$ that doesn't commute with the whole of R. Then clearly the map $\phi : x \mapsto rxr^{-1}$ gives a nontrivial automorphism of R. □

When R is commutative we first consider the case of odd sized component subring R_{odd} of R.

Classification of R_{odd}. We will show that indecomposable *components* of a rigid commutative odd-sized ring R_{odd} are isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$, for some odd prime p:

Claim 7.5. *If R_{odd} is an indecomposable rigid commutative odd-sized ring then $\exists$ prime p and $m \in \mathbb{N}$ such that, $R_{odd} \cong \mathbb{Z}/p^m\mathbb{Z}$.*

Proof (Claim 7.5). It is known (McDonald 1974) that any indecomposable commutative ring R_{odd} contains an associated *Galois ring* G such that:

$$G = (\mathbb{Z}/p^m\mathbb{Z})[x]/\big(f(x)\big)\,,$$

where $f(x)$ is square-free and irreducible over $\mathbb{Z}/p\mathbb{Z}$ and,

$$R_{odd} = G[x_1, \ldots, x_k]/(x_1^{n_1}, \ldots, x_k^{n_k}, g_1, \ldots, g_\ell)\,,$$

where $x_1, \ldots, x_k$ form an irredundant generating set for R_{odd} over G and the g_i's are polynomials in $(x_1, \ldots, x_k)$.

Let $\mathcal{M}$ be the ring generated by $x_1, \ldots, x_k$. This is an ideal of R_{odd}, it will be nonzero if we assume $k \geq 1$. Let $t > 0$ be the least integer such that $\mathcal{M}^t = 0$.

Consider the case when $t > 2$. We can assume without loss of generality that x_1 cannot be expressed as a polynomial in $x_2, \dots, x_k$ in the ring R_{odd}. Now choose an $\alpha \in \mathcal{M}^{t-1}$ such that no term in α is linear in x_1 and consider the map:

$$\phi : \begin{cases} x_1 & \mapsto x_1 + \alpha \\ x_2 & \mapsto x_2 \\ & \vdots \\ x_k & \mapsto x_k \end{cases}$$

ϕ is injective: otherwise a polynomial $h(x_1, \dots, x_k)$ maps to 0, in R_{odd}, under ϕ. This means that $h(x_1{+}\alpha, \dots, x_k){=}\ 0$ in R_{odd}. Now if $h(x_1, \dots, x_k)$ had no linear occurrence of x_1 then $h(x_1{+}\alpha, x_2, \dots, x_k){=}\ 0$ implies $h(x_1, \dots, x_k){=}\ 0$ (as $\alpha \cdot \mathcal{M} = 0$). On the other hand if $h(x_1, \dots, x_k)$ has a linearly occurring x_1 then $h(x_1 + \alpha, x_2, \dots, x_k) = 0$ implies that $x_1 =$(an expression containing no linear term in x_1). This combined with $x_1^{n_1} = 0$ means that $x_1 = 0$ which is a contradiction.

ϕ is onto: it is enough to show that in the ring R_{odd} we can obtain x_1 from $x_1 + \alpha, x_2, \dots, x_k$. Since α is generated by $x_1, \dots, x_k$ it can be expressed as a polynomial in $x_1, \dots, x_k$. Let $\alpha = x_1 \cdot h(x_1, \dots, x_k) + g(x_2, \dots, x_k)$, where $h(x_1, \dots, x_k)$ has no constant term. Then

$$\begin{aligned} x_1 + \alpha - g(x_2, \dots, x_k) &= x_1 + x_1 \cdot h(x_1, \dots, x_k) \\ &= x_1 + x_1 \cdot h(x_1 + \alpha, x_2, \dots, x_k) \quad (\text{as } \alpha \cdot \mathcal{M} = 0) \\ &= x_1 \cdot \big(1 + h(x_1 + \alpha, x_2, \dots, x_k)\big) \,. \end{aligned}$$

Now $h(x_1 + \alpha, x_2, \dots, x_k) \in \mathcal{M}$, and therefore by the property of local rings, $(1 + h(x_1 + \alpha, x_2, \dots, x_k))$ has to be invertible in R_{odd} and thus,

$$x_1 = \big[(x_1 + \alpha) - g(x_2, \dots, x_k)\big] \cdot \big[1 + h(x_1 + \alpha, x_2, \dots, x_k)\big]^{-1} \quad \text{in } R_{odd} \,.$$

Thus, ϕ induces a nontrivial automorphism of R_{odd}. This means that for R_{odd} to be rigid, we must have that the number of variables k is zero implying that R is just a Galois ring – $R_{odd} = G$. If $f(x)$ is of degree > 1 then $(\mathbb{Z}/p\mathbb{Z})[x]/(f(x))$ has a nontrivial automorphism, the *Frobenius* automorphism sending $x \mapsto x^p$, which can be *Hensel lifted* (see Lemma 9.13) to a nontrivial automorphism of $(\mathbb{Z}/p^m\mathbb{Z})[x]/(f(x))$ too. Thus, the only way that R_{odd} has no nontrivial automorphism is when degree of $f(x)$ is 1 meaning $R_{odd} = G = \mathbb{Z}/p^m\mathbb{Z}$.

Now suppose $t = 2$. If $k \geq 2$ then taking $\alpha = x_2$ in the above discussion gives us a nontrivial automorphism ϕ of R_{odd}. If $k = 1$ then the map $\phi : x_1 \mapsto$

$2x_1$ is a nontrivial automorphism of R_{odd}. If $k = 0$ then $R_{odd} = G$ and as shown before the only way that R_{odd} has no nontrivial automorphism is when $R_{odd} = G = \mathbb{Z}/p^m\mathbb{Z}$.

The last case of $t = 1$ means $\mathcal{M} = 0$ implying $R_{odd} = G$ which as before yields $R_{odd} = G = \mathbb{Z}/p^m\mathbb{Z}$. □

As a consequence of the above observations we have that any rigid commutative odd-sized ring R_{odd} looks:

(7.6)
$\times_i \times_j \mathbb{Z}/p_i^{\alpha_{i,j}}\mathbb{Z}$ where, p_i's are distinct odd primes and $1 \leq \alpha_{i,1} < \alpha_{i,2} < \cdots$.

Classification of R_{2pow}. Let us now take up the case of the power-of-2 sized component subring R_{2pow} of R. We will show that R_{2pow} is rigid only if the indecomposable rings that appear in the decomposition of R_{2pow} are isomorphic to either $\mathbb{Z}/2^m\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$.

Claim 7.7. *If R_{2pow} is an indecomposable rigid commutative power-of-2 sized ring then R_{2pow} is either $\mathbb{Z}/2^m\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$.*

Proof (Claim 7.7). Recall the proof of the Claim 7.5. The only case which needs to be handled in the case of *even* sized ring is when $t = 2$ and $k = 1$. The rigidity of R_{2pow} implies that the characteristic of R_{2pow} is 2 for otherwise $\phi : x_1 \mapsto 3x_1$ gives a nontrivial automorphism of R_{2pow}. Thus, *the* rigid ring with $t = 2, k = 1$ is $R = (\mathbb{Z}/2\mathbb{Z})[x_1]/(x_1^2)$. □

It follows from the above claim that a commutative power-of-2 sized ring is rigid iff it is isomorphic to one of the following:

$$\begin{aligned}
&\mathbb{Z}/2^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/2^{\alpha_n}\mathbb{Z}\\
&\text{or}\\
&(\mathbb{Z}/2\mathbb{Z})[x]/(x^2) \times \mathbb{Z}/2^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/2^{\alpha_n}\mathbb{Z}\\
&\text{where, } 1 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_n.
\end{aligned} \tag{7.8}$$

Collecting these two classifications, we get the classification Theorem 7.2 for finite rigid rings.

□

7.2. The algorithm for RA. We now give the algorithm referred to in Theorem 7.1 for testing the rigidity of a ring. Our algorithm for RA will test whether a given ring R is of the form given in the classification Theorem 7.2

or not. As in the classification Theorem 7.2, suppose that the decomposition of a given input ring R is:

$$R = R_{2pow} \times R_{odd}\,, \tag{7.9}$$

where R_{2pow} is a power-of-2 sized ring and R_{odd} is an odd-sized ring. Note that since it is easy to factor out powers of 2 from any integer, we can compute the decomposition of the additive group $(R, +)$ of R as the direct sum of two subgroups – one having power-of-2 size and another having odd size. This decomposition of $(R, +)$ then readily gives a decomposition of the form (7.9) of the input ring R. Note that now R is rigid if and only if both R_{2pow} and R_{odd} are rigid rings. In this way our problem boils down into the cases – testing rigidity of R_{2pow} and that of R_{odd}.

Testing rigidity of R_{2pow}. Since we can factor polynomials over $\mathbb{Z}/2^m\mathbb{Z}$ we can compute the decomposition of R_{2pow} into indecomposable rings and check whether they are of the forms: $\mathbb{Z}/2^m\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$ or not. Hence, we can check the rigidity of power-of-2-sized rings in polynomial time.

Testing rigidity of R_{odd}. Let R_{odd} be given as:

$$(R_{odd}, +) = (\mathbb{Z}/m_1\mathbb{Z})e_1 \oplus \cdots \oplus (\mathbb{Z}/m_n\mathbb{Z})e_n\,.$$

Here we can assume that $(m_1, \ldots, m_n) = (d_1^{\alpha_{1,1}}, d_1^{\alpha_{1,2}}, \ldots, d_2^{\alpha_{2,1}}, d_2^{\alpha_{2,2}}, \ldots, d_t^{\alpha_{t,1}}, d_t^{\alpha_{t,2}}, \ldots)$ where $d_1, \ldots, d_t$ are mutually coprime. For otherwise $\exists i \neq j$ s.t. $gcd(m_i, m_j) =: g > 1$ and can be used to break m_i or m_j into coprime factors $a, b \in \mathbb{Z}^{>1}$, hence, breaking $(R_{odd}, +)$ further by applying:

$$\big((\mathbb{Z}/ab\mathbb{Z})e_k, +\big) \cong (\mathbb{Z}/a\mathbb{Z})(be_k) \oplus (\mathbb{Z}/b\mathbb{Z})(ae_k)\,.$$

We can repeatedly apply this process of refining the basis to get basis representations of the ring R_{odd} over:

$$\mathbb{Z}/d_1^{\alpha_{1,1}}\mathbb{Z} \oplus \mathbb{Z}/d_1^{\alpha_{1,2}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_2^{\alpha_{2,1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t^{\alpha_{t,1}}\mathbb{Z} \oplus \cdots$$

for some coprime $d_1, d_2, \ldots, d_t \in \mathbb{Z}^{>1}$.

Let us define for all $1 \leq i \leq t$,

$$R_i := \{r \in R_{odd} \mid r \text{ has a power-of-}d_i \text{ additive order}\}\,.$$

Now since the d_i's are mutually coprime $R_{odd} \cong \times_{i=1}^t R_i$ (as in the proof of Proposition 2.13). Thus, R_{odd} has a nontrivial automorphism iff $\exists i \in [t],\ R_i$

has a nontrivial automorphism. Consequently, we can assume without loss of generality that the additive basis of the rings R_{odd} is given in the form:

$$(R_{odd}, +) = (\mathbb{Z}/d^{\alpha_1}\mathbb{Z})e_1 \oplus \cdots \oplus (\mathbb{Z}/d^{\alpha_n}\mathbb{Z})e_n\,. \tag{7.10}$$

We can also assume that α_i's are distinct (say, $1 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_n$) otherwise R_{odd} would not be rigid as it would not be of the form in the classification Theorem 7.2. Thus, we need to check if a given ring R_{odd} is of the form:

$$\mathbb{Z}/d^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/d^{\alpha_n}\mathbb{Z}\,. \tag{7.11}$$

REMARK 7.12. *There do exist rings whose additive group is of the form* (7.10) *but the rings themselves are not of the form* (7.11). *For example, the ring* $R \overset{\text{def}}{=} (\mathbb{Z}/d^2\mathbb{Z})[x]/\langle x^2, dx\rangle$ *has additive group isomorphic to* $\mathbb{Z}/d^2\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z}$ *but* R *is* not *isomorphic to* $\mathbb{Z}/d^2\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$.

Overview of the algorithm. Now we sketch an algorithm to check whether R_{odd} is isomorphic to:

$$\mathbb{Z}/d^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/d^{\alpha_n}\mathbb{Z} \quad \text{for } \alpha_1 < \cdots < \alpha_n\,.$$

Our algorithm proceeds by decomposing R_{odd} into $\mathbb{Z}/d^{\alpha_1}\mathbb{Z} \times R'$ and then recursively verifying that the component ring R' is of the form

$$\mathbb{Z}/d^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/d^{\alpha_n}\mathbb{Z} \quad \text{for } \alpha_1 < \alpha_2 \cdots < \alpha_n\,.$$

The key observation behind obtaining the decomposition of R_{odd} into $\mathbb{Z}/d^{\alpha_1}\mathbb{Z} \times R'$ is the following claim which is easy to verify:

CLAIM 7.13. *If*

$$\psi : R_{odd} \to \mathbb{Z}/d^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/d^{\alpha_n}\mathbb{Z}$$

is an isomorphism and

$$(R_{odd}, +) = (\mathbb{Z}/d^{\alpha_1}\mathbb{Z})e_1 \oplus \cdots \oplus (\mathbb{Z}/d^{\alpha_n}\mathbb{Z})e_n\,,$$

then $\psi(e_1) = (\beta_1, \beta_2, \ldots, \beta_n)$ *where* $\beta_1 \in (\mathbb{Z}/d\mathbb{Z})^*$ *and* $d|\beta_2, \ldots, \beta_n$, *so that if* $f(x) \in \mathbb{Z}[x]$ *is the minimal polynomial of* e_1 *in* R_{odd} *then*

$$f(x)\ (mod\ d) = x^\ell \cdot \Big(x - \big(\beta_1\ (mod\ d)\big)\Big) \quad \textit{for some } \ell \in \mathbb{Z}^{\geq 0}\,.$$

Following the above claim, we compute $\beta_1 \in \mathbb{Z}/d^{\alpha_1}\mathbb{Z}$ and thereby obtain the zero divisor $(e_1 - \beta_1)$ of R_{odd} and this zero divisor is then used in the standard way to decompose R_{odd}.

Algorithm. To determine if R_{odd} is of the form (7.11).

S-1. Compute $f(x) :=$ minpoly of e_1 over $\mathbb{Z}/d^{\alpha_n}\mathbb{Z}$. This can be found out by checking whether e_1^i can be written as a linear combination of $1, e_1, \ldots, e_1^{i-1}$ which amounts to doing linear algebra (mod d^{α_n}).

S-2. If $R_{odd} \cong \mathbb{Z}/d^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/d^{\alpha_n}\mathbb{Z}$ then say $e_1 = (\beta_1, \ldots, \beta_n)$ where $\beta_i \in \mathbb{Z}/d^{\alpha_i}\mathbb{Z}$. Also, since e_1 has characteristic d^{α_1} and $\alpha_1 \lneq \alpha_2, \ldots, \alpha_n$ we can deduce: β_1 is coprime to d and $d|\beta_2, \ldots, \beta_n$.

These observations mean that:

$$\begin{aligned} f(x) &= \mathrm{lcm}_{i=1}^{n} \{\text{minpoly of } \beta_i \text{ over } \mathbb{Z}/d^{\alpha_i}\mathbb{Z}\} \\ &\equiv (x - \beta_1)x^l \pmod{d}, \quad \text{for some } l \in \mathbb{Z}^{\geq 0} \end{aligned}$$

or else R_{odd} is not of the form (7.11). So we have a non-repeating root $\beta_1 (\mathrm{mod}\ d)$ of $f(x) (\mathrm{mod}\ d)$ and we can use Hensel lifting (see Lemma 9.13) to find a root of $f(x) (\mathrm{mod}\ d^{\alpha_1})$, which gives $\beta_1 (\mathrm{mod}\ d^{\alpha_1})$.

S-3. Consider $e_1 - \beta_1 = (0, \beta_2 - \beta_1, \ldots, \beta_n - \beta_1)$. Note that $\beta_2 - \beta_1, \ldots, \beta_n - \beta_1$ are all coprime to d. So if we compute (using linear algebra)

$$R_1 := \left\{\gamma \in R_{odd} \mid (e_1 - \beta_1)\gamma = 0\right\},$$

then $R_1 \cong \mathbb{Z}/d^{\alpha_1}\mathbb{Z}$ or else R_{odd} is not of the form (7.11).

S-4. Let $\hat{e}_1 \in R_{odd}$ be the unity of R_1. Compute $R_1^{\perp} := \{\gamma \in R_{odd} \mid \hat{e}_1\gamma = 0\}$. Check that $R_{odd} = R_1 \times R_1^{\perp}$ otherwise R_{odd} is not of the form (7.11).

S-5. Recursively check whether $R_1^{\perp} \cong \mathbb{Z}/d^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/d^{\alpha_n}\mathbb{Z}$ or not.

8. The complexity of finding a nontrivial ring automorphism

We just saw that deciding whether a ring has a nontrivial automorphism is in P. Here, we give evidence that the search version of this problem is apparently harder. We show that FRA is as (randomly) hard as Integer Factoring (IF). We also show that if FRA is in P then Polynomial Factoring is also in P (assuming the ERH).

8.1. Reduction from integer factoring to FRA.

THEOREM 8.1. *IF* $\equiv_T^{ZPP}$ *FRA*.

PROOF. Let us first see how we can find a nontrivial ring automorphism if we can do integer factoring. Suppose the given ring R is non-commutative then we know from the proof of Claim 7.4: there is a *unit* of R that does not commute with the whole of R and thus defines a nontrivial automorphism. So we compute the multiplicative generators of R^* in *randomized* polynomial time and surely one of the generators will not commute with the whole of ring R.

Now assume the given ring R is commutative. It can be decomposed into local rings, as remarked after Proposition 2.15, in expected polynomial time using randomized methods for polynomial factorization and oracle of integer factorization. Once we have local rings we can output nontrivial automorphisms like ϕ in the proof of Claim 7.5.

Conversely, suppose we can find nontrivial automorphisms of rings and n is a given number. We can assume that n has no small ($\leq (\log n)^3$) prime factor p for clearly we can find such small prime factors in polynomial-time. Let $n = p^a \cdot m$ where, p^a is the highest power of the prime p which divides n and m is coprime to p. Randomly choose a monic cubic polynomial $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$. Define $R := (\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$ and suppose we can find a nontrivial automorphism ϕ of R. It follows from the distribution of irreducible polynomials over finite fields (Lidl & Niederreiter 1994) that with probability $\sim \frac{1}{9}$, $f \pmod n$ satisfies the following properties:

- $f(\mathrm{mod}\ n)$ is squarefree. Equivalently, n is coprime to the discriminant, Δ_f, of f.
- $f(\mathrm{mod}\ m)$ is irreducible. That is, there exists a prime $q|m$ such that $f(\mathrm{mod}\ q)$ is irreducible.
- $f(\mathrm{mod}\ p)$ has exactly two irreducible factors f_1, f_2, say f_1 is linear.

Thus,

$$R \cong (\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/p^a\mathbb{Z})[x]/\big(f_2(x)\big) \times (\mathbb{Z}/m\mathbb{Z})[x]/\big(f(x)\big)\,.$$

Note that we can compute R^ϕ, the set of elements of R fixed by ϕ, using linear algebra (if at any point we cannot invert an element (mod n), we get a factor of n). As ϕ is a nontrivial automorphism of R we have that ϕ is identity on atmost one of the component rings $(\mathbb{Z}/p^a\mathbb{Z})[x]/(f_2(x))$ or $(\mathbb{Z}/m\mathbb{Z})[x]/(f(x))$. Thus, we have three cases:

C-1). If ϕ fixes $(\mathbb{Z}/p^a\mathbb{Z})[x]/(f_2(x))$:
Then $R^\phi \cong (\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/p^a\mathbb{Z})[x]/(f_2(x)) \times ((\mathbb{Z}/m\mathbb{Z})[x]/(f(x)))^\phi$. Thus, $|R^\phi| = p^{3a}m_1$ where $m_1 \neq m^3$ as ϕ moves $(\mathbb{Z}/m\mathbb{Z}/(f(x)))$.

C-2). If ϕ fixes $(\mathbb{Z}/m\mathbb{Z})[x]/(f(x))$:
Then $R^\phi \cong (\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})[x]/(f(x))$. Thus, $|R^\phi| = p^{2a}m^3$.

C-3). If ϕ moves both $(\mathbb{Z}/p^a\mathbb{Z})[x]/(f_2(x))$ and $(\mathbb{Z}/m\mathbb{Z})[x]/(f(x))$:
Then $R^\phi \cong (\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})[x]/(f(x))^\phi$. Thus, $|R^\phi| = p^{2a} \cdot m_1$, where $m_1 \neq m^2$ because $f(\bmod\ m)$ is irreducible. (if q is a prime such that $q^b|m$ and $f(\bmod\ q)$ is irreducible, then $(\mathbb{Z}/q^b\mathbb{Z})[x]/(f(x))^\phi$ has size precisely q^b.)

Since, the size of R^ϕ is in no case of the form n, n^2 or n^3, the process of finding R^ϕ by doing linear algebra (mod n) is going to yield a factor of n. In particular, this means that if the matrix describing ϕ over the natural additive basis $\{1, x, x^2\}$ is:

$$A := \begin{pmatrix} 1 & 0 & 0 \\ a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix},$$

then the determinant of one of the submatrices of $(A - I)$ will have a nontrivial gcd with n.

Thus, the two problems: finding nontrivial automorphisms of commutative rings and integer factoring have the same complexity (with respect to randomized polynomial time reductions). □

8.2. Reduction from polynomial factoring to FRA. Polynomial factorization over finite fields is still not known to have a deterministic polynomial time algorithm. The randomized algorithms known for this problem (Gathen & Gerhard 1999; Lidl & Niederreiter 1994) invariably use automorphisms of rings as a tool (Agrawal & Saxena 2005).

Here, we give a specific relation of polynomial factorization to FRA assuming the extended Riemann hypothesis (ERH). ERH needs to be invoked as it gives us a deterministic polynomial time algorithm to find k^{th} roots in a finite field (Gathen & Gerhard 1999). The reduction we give here uses the main idea of Evdokimov's algorithm (Evdokimov 1994).

Theorem 8.2. *Assuming the ERH, Polynomial Factoring $\leq_m^P$ FRA.*

Proof. Suppose we want to factor a polynomial $f(x)$ over the finite field $\mathbb{F}_q$. We could assume wlog that $f(x)$ is square free and splits completely over $\mathbb{F}_q$. Let us define a ring $R := \mathbb{F}_q[x]/(f(x))$ and let d be the degree of $f(x)$. Suppose an oracle of FRA gives a nontrivial automorphism ϕ of the ring R. We will show how to find a factor of $f(x)$ assuming ERH.

We can first easily compute the subring R^ϕ of elements in R which are fixed by ϕ. If $x, \phi(x), \phi^2(x), \ldots, \phi^d(x)$ are all distinct modulo $f(x)$ then we have $(d+1)$ roots of degree-d-polynomial $f(x)$ which implies that $\exists i \neq j$ *s.t.* $gcd(\phi^i(x) - \phi^j(x), f(x))$ factors $f(x)$. So we can assume that for some $2 \leq k \leq d$, $\phi^k(x) = x$.

Let us now invoke ERH and assume that we have a k-th root of unity $\zeta_k \in \mathbb{F}_q$. Consider the element:

$$\beta := \sum_{i=0}^{k-1} \zeta_k^i \phi^i(x) \in R,$$

which satisfies $\phi(\beta) = \zeta_k^{-1}\beta$. Thus, $\beta^k \in R^\phi$ but $\beta \notin R^\phi$. Also, note that β^k has a k-th root y in the ring R^ϕ for β^k has a k-th root in $R \cong \bigotimes_{i=1}^d \mathbb{F}_q$ and R^ϕ is just a subring of R where we impose equality constraints on some of the components. Also, we can compute $y \in R^\phi$ as we are assuming ERH (the k-th root finding algorithm either gives a k-th root of β^k in R^ϕ *or* factors $f(x)$). But then we have $(k+1)$ k-th roots of β^k which are all distinct modulo $f(x)$, namely: $\beta, \zeta_k\beta, \ldots, \zeta_k^{k-1}\beta, y$; thus, the difference of two of these roots is a zero divisor of the ring R and hence will have a nontrivial *gcd* with $f(x)$. □

9. Conclusion and open problems

Figure 9.1 shows the various relations we proved in this paper. The arrows are labelled by the type of reduction or relation and the dotted arrow signifies a conditional result (assuming ERH). The well-known problems are in the central circle and labelled as: IF for integer factoring, GI for graph isomorphism and PF for polynomial factoring.

This paper studied the automorphism and isomorphism problems of rings. The problems were all inspired from those of graphs. The rings considered in this work were assumed to be finite which was used in showing that these problems are of intermediate complexity and unlikely to be NP-hard. This paper showed that the automorphism problems of finite rings are related to the classical problems – like, graph isomorphism, integer factoring and polynomial factoring – and the most general automorphism problem is computing the group of automorphisms of a finite ring.

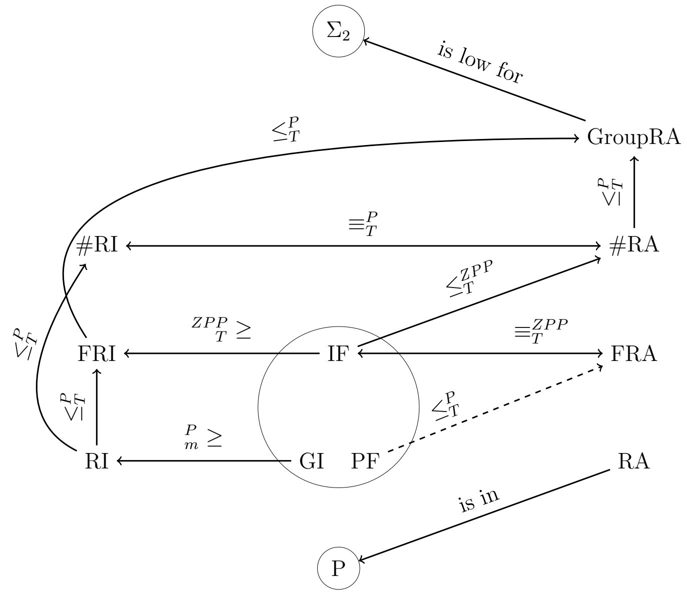

Figure 9.1: Relations among the Ring Morphism Problems.

The complexity of all the morphism problems, except RA and testing automorphism/isomorphism problems, that we considered in this paper remain open. A solution to any one of them will be very interesting as it would solve some of the classical problems as well! To understand these problems more we would like to ask the following questions:

- We have seen two well-known problems of intermediate complexity reduce to #RA. Can one reduce some other such problem, e.g., finding discrete logarithm?
- The ring problems differ from the graph ones in their (in)ability to efficiently "fix" part of the automorphisms. This property allows one to prove the equivalence between computing automorphism groups, counting automorphisms, finding isomorphisms, and testing isomorphisms in the case of graphs. For rings, we cannot prove such equivalence. Does there exist some way of doing such "fixing" for rings which will allow us to prove similar equivalences?
- As #RA is an algebraic problem is there a polynomial time quantum algorithm for it, i.e., is #RA $\in$ BQP?

- Consider the ring isomorphism problem over rationals: $\mathrm{RI}_{\mathbb{Q}}$. It is not even clear if this problem is decidable.

Appendix: Facts about rings

A *ring* is a set R equipped with two binary operations $+$ and $\cdot$, called addition and multiplication, such that (a, b, c are general elements in R):

1). $(R, +)$ is an *abelian group* with identity element 0:

- Associativity: $(a + b) + c = a + (b + c)$
- Commutativity: $a + b = b + a$
- Identity: $0 + a = a + 0 = a$
- Inverse: $\forall a\ \exists(-a)$ such that $a + -a = -a + a = 0$

2). $(R, \cdot)$ is a *monoid* with identity element 1:

- Identity: $1 \cdot a = a \cdot 1 = a$
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3). Multiplication distributes over addition:

- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

If $(R \setminus \{0\}, \cdot)$ is an abelian group too then R becomes a *field*.

EXAMPLE 9.1. $R_0 := (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring, it is a field iff n is prime. $R_1 := R_0[x]/(x^r - 1)$ is a commutative ring but never a field for $r > 1$. The set $R_2 := \left\{A \mid A \in R_0^{2\times 2}\right\}$ is a noncommutative ring under matrix addition and multiplication in R_0. ♢

We first collect some results related to decomposition of rings into simpler rings. A ring R is said to be *decomposable* if there are subrings R_1, R_2 such that:

- $R_1 \cdot R_2 = R_2 \cdot R_1 = 0$, i.e., for all $r_1 \in R_1, r_2 \in R_2$, $r_1 \cdot r_2 = r_2 \cdot r_1 = 0$.
- $R_1 \cap R_2 = \{0\}$.
- $R = R_1 + R_2$, i.e., for every $r \in R$ there are $r_1 \in R_1, r_2 \in R_2$ such that $r = r_1 + r_2$.

Such a ring decomposition has been denoted by $R = R_1 \times R_2$ in this work. The subrings R_1, R_2 are called *component* rings of R.

Example 9.2. The ring $R := \mathbb{F}[x]/(x^2 - x)$ decomposes as: $R = Rx \times R(1 - x) \cong \mathbb{F} \times \mathbb{F}$. Here, Rx is a short-hand for the set $\{r \cdot x \mid r \in R\}$. Note that $Rx, R(1-x)$ are subrings of R and have $x, (1-x)$ as their (multiplicative) identity elements respectively. ◊

An element $r \in R$ is called an *idempotent* if $r^2 = r$. The following lemma shows how idempotents help in decomposing a commutative ring.

Lemma 9.3. *A commutative ring R decomposes iff R has an idempotent element other than* $0, 1$.

Proof. Suppose $R = R_1 \times R_2$ is a nontrivial decomposition and let the identity element 1 of R be expressible as $1 = s + t$ where $s \in R_1, t \in R_2$. Then by the definition of decomposition we have:

$$\begin{aligned} & 1 \cdot 1 = (s+t) \cdot (s+t) \\ \Rightarrow\quad & 1 = s^2 + t^2 \qquad [\because s \cdot t = 0] \\ \Rightarrow\quad & s + t = s^2 + t^2 \\ \Rightarrow\quad & s - s^2 = t^2 - t \\ \Rightarrow\quad & s - s^2 = 0 \qquad \left[\because s - s^2 \in R_1 \cap R_2 = \{0\}\right] \\ \Rightarrow\quad & s \text{ is an idempotent.} \end{aligned}$$

Note that if $s = 0$ then $t = 1$ and then $R_1 = 0$ (as for all $r_1 \in R_1,\ r_1 \cdot R_2 = 0$) and similarly, if $s = 1$ then $R_2 = 0$. As R_1, R_2 are nonzero subrings of R we deduce that $s \neq 0, 1$ and hence s is an idempotent other than $0, 1$.

Conversely, suppose that $s \neq 0, 1$ is an idempotent of R. Then consider the subrings $R \cdot s$ and $R \cdot (1 - s)$. Note that $s, (1-s)$ are the identity elements of $Rs, R(1-s)$ respectively. For any two elements $rs \in Rs, r'(1-s) \in R(1-s)$: $rs \cdot r'(1-s) = rr'(s - s^2) = 0$. If $r \in Rs \cap R(1-s)$ then $rs = 0$ and $r(1-s) = 0$ implying that $r = 0$. Finally, we can express any $r \in R$ as: $r = rs + r(1-s)$. Thus, R decomposes as: $R = Rs \times R(1-s)$. □

The following lemma shows that a decomposition of a ring into indecomposable rings is unique.

Lemma 9.4. *Let R be a ring and $R_1, \ldots, R_k$ be indecomposable nonzero rings such that:*

$$R = R_1 \times R_2 \times \cdots \times R_k\,.$$

Then this decomposition is unique up to ordering, i.e., if we have indecomposable nonzero S_j's such that:

$$R = R_1 \times \cdots \times R_k = S_1 \times \cdots \times S_l\,,$$

then $k = l$ and there exists a permutation π such that for all $i \in [k]$, $\quad R_i = S_{\pi(i)}$.

Proof. Assume wlog that $k \geq l$. Let ϕ_1 be a homomorphism of the ring R such that ϕ_1 is identity on S_1 and $\phi_1(S_2) = \cdots = \phi_1(S_l) = 0$. ϕ_1 is well defined simply because $R = S_1 \times \cdots \times S_l$.

Clearly, $\phi_1(R_1), \phi_1(R_2), \ldots, \phi_1(R_k)$ are all subrings of S_1 and:

$$\phi_1(R) = \phi_1(R_1) + \phi_1(R_2) + \cdots + \phi_1(R_k) = S_1.$$

Can these subrings have nontrivial intersection? Say, $s_1 \in \phi_1(R_i) \cap \phi_1(R_j)$ for some $i \neq j$ then there are some $s, s' \in S_2 + \cdots + S_l$ such that $s_1 + s \in R_i$ and $s_1 + s' \in R_j$. Let a be the (multiplicative) identity of $R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_k$ and b be the identity of R_i. Then:

$$\begin{aligned}
& (s_1 + s)a = 0 \text{ and } (s_1 + s')b = 0 \quad [\because R = R_1 \times \cdots \times R_k] \\
\Rightarrow\quad & (s_1 + s)a + (s_1 + s')b = 0 \\
\Rightarrow\quad & s_1(a + b) + sa + s'b = 0 \\
\Rightarrow\quad & s_1 + (sa + s'b) = 0 \quad [\because 1 = a + b] \\
\Rightarrow\quad & s_1 = (sa + s'b) = 0 \quad [\because s_1 \in S_1 \text{ and } sa, s'b \in S_2 + \cdots + S_l] \\
\Rightarrow\quad & \phi_1(R_i) \cap \phi_1(R_j) = \{0\} \text{ for all } i \neq j \in [k].
\end{aligned}$$

Also, for any $r_i \in R_i, r_j \in R_j, \quad r_i r_j = 0$ implying that $\phi_1(r_i) \cdot \phi_1(r_j) = 0$. The properties above together mean that:

$$S_1 = \phi_1(R_1) \times \phi_1(R_2) \times \cdots \times \phi_1(R_k)\,.$$

Since S_1 was assumed to be indecomposable we have that exactly one of the subrings above is nonzero. Wlog say, $\phi_1(R_2) = \cdots = \phi_1(R_k) = 0$ and then it is implied that $\phi_1(R_1) = S_1$.

Similarly, we can define ϕ_i to be a homomorphism of the ring R such that ϕ_i is identity on S_i and $\phi_i(S_j) = 0$ for all $j \in [l] \setminus \{i\}$. Then the above argument says that there is an injective map $\tau : [l] \to [k]$ such that for all $i \in [l]$:

$$\phi_i(R_{\tau(i)}) = S_i \quad \text{and} \quad \phi_i(R_j) = 0 \quad \text{for all} \quad j \in [k] \setminus \{\tau(i)\}\,. \tag{9.5}$$

Now consider an $l \times k$ matrix $D = ((\delta_{i,j}))$ where $\delta_{i,j} = 1$ if $\phi_i(R_j) = S_i$ else $\delta_{i,j} = 0$. Equation (9.5) tells us that each row of D has exactly one 1. Now if $k > l$ then D has more columns than rows and hence there is a zero column, say j-th, implying that $\phi_i(R_j) = 0$ for all $i \in [l]$. But this means that $R_j = 0$ which is a contradiction. Hence, $k = l$ and D has exactly one 1 in each row and column, thus making τ a permutation.

So now we have that for any $j \in [k]$, $\quad \phi_{\tau^{-1}(j)}(R_j) = S_{\tau^{-1}(j)}$ and $\phi_i(R_j) = 0$ for all $i \in [k] \setminus \{\tau^{-1}(j)\}$. In other words for any $j \in [k]$, $\quad R_j = S_{\tau^{-1}(j)}$.

This completes the proof of unique decomposition of rings into indecomposable subrings. □

So what is the structure of these indecomposable rings that appear in the decomposition? Here, we sketch the form of indecomposable rings that are finite and commutative.

Lemma 9.6. *Let R be a finite commutative indecomposable ring. Then,*

(i) R has a prime-power characteristic, say p^m for some prime p.

(ii) R can be expressed in the form:

$$R = \Big((\mathbb{Z}/p^m\mathbb{Z})[z]/\big(h(z)\big)\Big)[y_1, \ldots, y_k]/\big(y_1^{e_1}, \ldots, y_k^{e_k}, h_1(z, y_1, \ldots, y_k), \ldots, \\ \ldots, h_l(z, y_1, \ldots, y_k)\big)\,,$$

where $h(z)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$ and h_i's are multivariate polynomials over $\mathbb{Z}/p^m\mathbb{Z}$.

Remark 9.7. *The ring $(\mathbb{Z}/p^m\mathbb{Z})[z]/(h(z))$, where $h(z)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$, is called* Galois ring. *It is a finite field if $m = 1$.*

Notice that the form of R claimed in (ii) above says that the generators $y_1, \ldots, y_k$ of R are nilpotents, *i.e., they vanish when raised by a suitable integer.*

Proof (i). Suppose R is a finite commutative indecomposable ring with characteristic n. If n nontrivially factors as: $n = ab$, where $a, b \in \mathbb{Z}^{>1}$ are coprime, then by Chinese remaindering R factors too:

$$R = aR \times bR\,.$$

(Convince yourself that this is a decomposition.) This contradiction shows that n is a prime power, say $n = p^m$. □

Proof (ii). We assume $m = 1$ for simplicity of exposition. These ideas carry forward to larger m's (McDonald 1974). So suppose that R is an $\mathbb{F}_p$-algebra and is given in terms of basis elements $b_1, \ldots, b_n$. Let $g_1(b_1, \ldots, b_n), \ldots, g_l(b_1, \ldots, b_n)$ be the multivariate polynomials that define the multiplication operation of the ring R. Thus, we have an expression for R as:

$$R \cong \mathbb{F}_p[x_1, \ldots, x_n]/\big(g_1(x_1, \ldots, x_n), \ldots, g_l(x_1, \ldots, x_n)\big)\,. \tag{9.8}$$

Since R is of dimension n, $\{1, x_1, x_1^2, \ldots, x_1^n\}$ cannot all be linearly independent and hence there is a polynomial $f_1(z) \in \mathbb{F}_p[z]$ of degree atmost n such that $f_1(x_1) = 0$ in R. Further, assume that f_1 is of lowest degree. Now if f_1 nontrivially factors as: $f_1(z) = f_{11}(z)f_{12}(z)$, where f_{11}, f_{12} are coprime, then by Chinese remaindering R decomposes as:

$$R \cong R \cdot f_{11}(x_1) \times R \cdot f_{12}(x_1)\,.$$

As R is assumed to be indecomposable we deduce that f_1 is a power of an irreducible polynomial. Say, $f_1(z) = f_{11}(z)^{e_1}$ where f_{11} is an irreducible polynomial over $\mathbb{F}_p$ of degree d_1. Now we claim that there are $g_1', \ldots, g_l' \in \mathbb{F}_{p^{d_1}}[x_1, \ldots, x_n]$ such that:

$$R \cong \mathbb{F}_{p^{d_1}}[x_1, \ldots, x_n]/\big(x_1^{e_1}, g_1'(x_1, \ldots, x_n), \ldots, g_l'(x_1, \ldots, x_n)\big)\,. \tag{9.9}$$

To prove the above claim we need the following fact:

Claim 9.10. *If $f(x)$ is an irreducible polynomial, of degree d, over a finite field $\mathbb{F}_q$ then*

$$S = \mathbb{F}_q[x]/\big(f(x)^e\big) \cong \mathbb{F}_{q^d}[u]/(u^e)\,.$$

Proof (Claim 9.10). Consider the ring $S' := (\mathbb{F}_q[x]/(f(x)))[u]/(u^e) \cong \mathbb{F}_{q^d}[u]/(u^e)$. We claim that the map $\phi : S \to S'$ which fixes $\mathbb{F}_q$ and maps $x \mapsto (x + u)$, is an isomorphism.

Note that $f(x+u)^e = 0$ in the ring S' simply because $f(x+u)-f(x) = u \cdot q(x)$ for some $q(x) \in \mathbb{F}_q[x]$. Thus, ϕ is a ring homomorphism from S to S'. Next we show that the minimum polynomial that $\phi(x)$ satisfies over S' is of degree de, thus the dimension of $\phi(S)$ is the same as that of S' over $\mathbb{F}_q$ and hence ϕ is an isomorphism.

Suppose $g(z) := \sum_{j=0}^{d'} a_j x^j$ is the least degree polynomial over $\mathbb{F}_q$ such that $g(x + u) = 0$ in S'. This means that in S':

$$0 = g(x + u) = g(x) + u \cdot g^{(1)}(x) + u^2 \cdot \frac{g^{(2)}(x)}{2!} + \cdots + u^{e-1} \cdot \frac{g^{(e-1)}(x)}{(e-1)!}\,,$$

where $\frac{g^{(i)}(x)}{i!} = \sum_{j=i}^{d'} \frac{j(j-1)\cdots(j-i+1)}{i!} a_j x^{j-i}$. But since $1, u, \dots, u^{e-1}$ are linearly independent over $\mathbb{F}_q[x]/(f(x))$. We have:

$$g(x) = g^{(1)}(x) = \cdots = g^{(e-1)}(x) = 0 \quad \text{over} \quad \mathbb{F}_q[x]/\big(f(x)\big)\,.$$

Whence we get, $f(z)^e | g(z)$ which by the definition of g means that $g(z) = f(z)^e$. Thus, ϕ is an isomorphism from S to S'. □

From the above claim we now deduce:

$$\begin{aligned} R &\cong \mathbb{F}_p[x_1, \dots, x_n]/\big(f_{11}(x_1)^{e_1}, g_1(x_1, \dots, x_n), \dots, g_l(x_1, \dots, x_n)\big) \\ &\cong \mathbb{F}_{p^{d_1}}[u, x_2, \dots, x_n]/\big(u^{e_1}, g_1'(u, x_2, \dots, x_n), \dots, g_l'(u, x_2, \dots, x_n)\big) \\ &\cong \mathbb{F}_{p^{d_1}}[x_1, x_2, \dots, x_n]/\big(x_1^{e_1}, g_1'(x_1, x_2, \dots, x_n), \dots, g_l'(x_1, x_2, \dots, x_n)\big)\,. \end{aligned}$$

This new ring which we obtained has x_1 as a nilpotent. We can now consider the lowest degree polynomial $f_2(z) \in \mathbb{F}_{p^{d_1}}[z]$ such that $f_2(x_2) = 0$ in R. The above process when repeated on f_2, x_2 in place of f_1, x_1 gives us that there are $d_2, e_2 \in \mathbb{Z}^{\geq 1}$ and $g_1'', \dots, g_l'' \in \mathbb{F}_{p^{d_1 d_2}}[x_1, \dots, x_n]$ such that:

$$R \cong \mathbb{F}_{p^{d_1 d_2}}[x_1, \dots, x_n]/\big(x_1^{e_1}, x_2^{e_2}, g_1''(x_1, \dots, x_n), \dots, g_l''(x_1, \dots, x_n)\big)\,.$$

Continuing this way we get that there is a $d \in \mathbb{Z}^{\geq 1}$ and polynomials $h_1, \dots, h_l \in \mathbb{F}_{p^d}[x_1, x_2, \dots, x_n]$ such that:

$$R \cong \mathbb{F}_{p^d}[x_1, \dots, x_n]/\big(x_1^{e_1}, \dots, x_n^{e_n}, h_1(x_1, \dots, x_n), \dots, h_l(x_1, \dots, x_n)\big)\,. \qquad \square$$

Remark 9.11. *Note that the above proof can be viewed as an algorithm to decompose a finite dimensional commutative ring, given in basis form, into indecomposable rings. It is indeed a deterministic polynomial time algorithm given oracles to integer and polynomial factorization.*

Let us now see a structural property of commutative indecomposable rings.

Lemma 9.12. *For a field $\mathbb{F}$, consider a ring R of the form:*

$$R = \mathbb{F}[x_1, \dots, x_n]/\big(x_1^{e_1}, \dots, x_n^{e_n}, h_1(x_1, \dots, x_n), \dots, h_\ell(x_1, \dots, x_n)\big)\,.$$

Then,

(i) R is indecomposable.

(ii) R has a unique maximal ideal $\mathcal{M}$ and $\mathcal{M} =$ set of nilpotents of R.

Proof (i). Any element r of R looks like $a_0 + a_1(\overline{x})x_1 + \cdots + a_n(\overline{x})x_n$ where, $a_0 \in \mathbb{F}$ and $a_1(\overline{x}), \ldots, a_n(\overline{x}) \in \mathbb{F}[x_1, \ldots, x_n]$.

Suppose $a_0 = 0$. Since, $x_1^{e_1} = \cdots = x_n^{e_n} = 0$ we have that:

$$\begin{aligned} r^{e_1+\cdots+e_n} &= \big(a_1(\overline{x})x_1 + \cdots + a_n(\overline{x})x_n\big)^{e_1+\cdots+e_n} \\ &= 0\,. \end{aligned}$$

Suppose $a_0 \neq 0$. Let $r_0 := r - a_0$ and $e := e_1 + \cdots + e_n$. Then we have:

$$\begin{aligned} (a_0 + r_0)\big(a_0^e - a_0^{e-1}r_0 + \cdots + (-1)^{e-1}a_0r_0^{e-1} + (-1)^e r_0^e\big) &= a_0^{e+1} - (-r_0)^{e+1} \\ &= a_0^{e+1} \qquad [\because r_0^e = 0] \\ &\in \mathbb{F}^* \\ &\Rightarrow r \in R^*\,. \end{aligned}$$

Thus, every element r of R is either a nilpotent or a unit depending upon whether $a_0 = 0$ or not.

Now suppose R is decomposable. By Lemma 9.3 there has to be a nontrivial idempotent $t \in R$. But we have:

$$\begin{aligned} & t^2 = t \\ \Rightarrow\quad & t(t-1) = 0 \\ \Rightarrow\quad & t = 0 \text{ or } 1 \qquad \big[\because t \text{ or } (t-1) \text{ is a unit}\big]\,. \end{aligned}$$

This contradiction shows that R is indecomposable. □

Proof (ii). Define a set $\mathcal{M} := R \setminus R^*$. As shown above $\mathcal{M}$ is the set of nilpotents of R and hence is an ideal. $\mathcal{M}$ is maximal because any element outside it is a unit. $\mathcal{M}$ is unique because it contains all the non-units of R. □

Suppose R is a ring, $\mathcal{I}$ is an ideal of R and $f \in R[z]$. Then a factorization of $f(z)$ modulo $\mathcal{I}$ can be "lifted" to one modulo $\mathcal{I}^2$ by a well known trick in algebra called *Hensel's Lifting.* This is a useful trick in many situations, for example, given a root of $f(x)$ modulo p we can lift it to a root of $f(x)$ modulo p^2.

Lemma 9.13 (Hensel's Lifting). *Let R be a ring and $\mathcal{I}$ be an ideal. Let $f(z) \in R[z]$ and $f = gh$ (mod $\mathcal{I}$) be a factorization of f over $R/\mathcal{I}$ such that there exists $a, b \in R[z]$, $ag + bh = 1$ (mod $\mathcal{I}$). Then,*

- *There are easily computable $g^*, h^*, a^*, b^* \in R[z]$ satisfying:*

$$\begin{aligned} &f = g^*h^* \ (mod\, \mathcal{I}^2) \\ &g^* = g \ (mod\, \mathcal{I}) \text{ and } h^* = h \ (mod\, \mathcal{I}) \\ &a^*g^* + b^*h^* = 1 \ (mod\, \mathcal{I}^2). \end{aligned}$$

- *Also, g^*, h^* above are unique in the sense that for any other g', h' satisfying the above conditions we have some $u \in \mathcal{I}$ such that:*

$$\begin{aligned} g' &= g^*(1+u) \ (mod\, \mathcal{I}^2) \\ h' &= h^*(1-u) \ (mod\, \mathcal{I}^2). \end{aligned}$$

Proof. See Lidl & Niederreiter (1994) for the proof. □

The following lemma lists two useful results regarding the polynomial hierarchy (PH): BPP is low for Σ_2 and the Swapping lemma.

Lemma 9.14. ◦ $\Sigma_2^{BPP} = \Sigma_2$.

- *Let M be a polynomial time deterministic Turing machine then for any positive constant c there is a positive c' such that:*

$$\begin{aligned} L &= \left\{x \mid \ Prob_{y\in\{0,1\}^c}\Big[\big(\exists z \in \{0,1\}^c\big) \ M(x,y,z) \ accepts\Big] \geq \frac{2}{3}\right\} \\ &= \left\{x \mid \ \big(\exists z \in \{0,1\}^c\big) Prob_{y\in\{0,1\}^{c'}}\big[M(x,y,z) \ accepts\big] \geq \frac{2}{3}\right\} \end{aligned}$$

Proof. See Schöning (1988). □

Acknowledgements

This work was done while the authors were visiting Princeton University, Princeton, NJ, USA in 2003-04. It was also partially supported by research funding from Infosys Technologies Limited, Bangalore and NUS, Singapore.

We would like to thank Manindra Agrawal, Hendrik Lenstra and Shien Jin Ong for many useful discussions. We especially thank Manindra Agrawal for lots of suggestions that made the paper readable. We thank Hendrik Lenstra for pointing out that **RA** $\in$ P even for noncommutative finite rings. We thank Stefan Staiger and Volker Diekert for pointing out corrections to the proof of Claim 7.5 in a preliminary version of this paper. We also want to thank anonymous referees for suggesting many changes to the preliminary version.

References

M. Agrawal & N. Saxena (2005). Automorphisms of Finite Rings and Applications to Complexity of Problems. In *22nd Annual Symposium on Theoretical Aspects of Computer Science, 2005*, 1–17.

M. Agrawal & N. Saxena (2006). Equivalence of F-Algebras and Cubic Forms. In *23rd Annual Symposium on Theoretical Aspects of Computer Science, 2006*, 115–126.

V. Arvind & J. Torán (2004). Solvable Group Isomorphism is (almost) in NP intersect coNP. In *19th Annual IEEE Conference on Computational Complexity, 2004*, 91–103.

L. Babai & E. Szemerédi (1984). On the complexity of matrix group problems. In *25th Annual IEEE Symposium on Foundations of Computer Science, 1984*, 229–240.

R. Boppana, J. Håstad & S. Zachos (1987). Does coNP have short interactive proofs? *Information Processing Letters* **25**(2), 127–132.

S. A. Evdokimov (1994). Factorization of polynomials over finite fields in subexponential time under GRH. In *1st International Symposium on Algorithmic Number Theory, 1994*, 209–219.

É. Galois (1846). Oeuvres mathématiques. *Journal des mathématiques pures et appliqués* **11**, 381–444.

J. Gathen & J. Gerhard (1999). *Modern Computer Algebra.* Cambridge University Press, Cambridge.

O. Goldreich & A. Wigderson (2002). Derandomization That Is Rarely Wrong from Short Advice That Is Typically Good. In *6th International Workshop on Randomization and Approximation Techniques, 2002*, 209–223.

S. Goldwasser, S. Micali & C. Rackoff (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing* **18**(1), 186–208.

S. Lang (1994). *Algebra.* Reading (MA): Addison-Wesley, 3rd edition.

H. Lenstra (2004). Private Communication, 2004.

R. Lidl & H. Niederreiter (1994). *Introduction to finite fields and their applications.* Cambridge University Press.

K. Manders & L. Adleman (1976). *NP*-complete decision problems for quadratic polynomials. In *8th Annual ACM Symposium on Theory of Computing, 1976*, 23–29.

B. R. McDonald (1974). *Finite Rings with Identity.* Marcel Dekker, New York.

G. L. Miller (1976). Riemann's Hypothesis and Tests for Primality. *Journal of Computer and System Sciences* **13**(3), 300–317.

M. I. Rosen (1995). Niels Hendrik Abel and equations of the fifth degree. *American Mathematical Monthly* **102**(6), 495–505.

U. Schöning (1988). Graph Isomorphism Is in the Low Hierarchy. *Journal of Computer and System Sciences* **37**(3), 312–323.

Manuscript received 14 September 2005

Neeraj Kayal
Institute for Advanced Study
Einstein Drive
Princeton, NJ 08540, USA
kayaln@ias.edu

Nitin Saxena
Centrum voor Wiskunde en Informatica
Kruislaan 413
1098 SJ, Amsterdam, The Netherlands
nitin.saxena@cwi.nl