SCIREA Journal of Mathematics
http://www.scirea.org/journal/Mathematics
February 12, 2022
Volume 7, Issue 1, February 2022
https://doi.org/10.54647/mathematics11310

A structure of Dedekind in the cryptosystem

Magdalena Jankowska, L ukasz Matysiak

Kazimierz Wielki University, Bydgoszcz, Poland

Email: magdalena.jankowska@student.ukw.edu.pl (Magdalena Jankowska),
lukmat@ukw.edu.pl (L ukasz Matysiak)

Abstract

In this paper we consider the structure of Dedekind in some developed cryptosystems. In one case, the structure exists with respect to a key, and in the other case, the structure exists with respect to two alphabets. The second part of this paper is an appendix that considers the applications of polynomial composites and monoid domains in cryptology.

Keywords: cryptology, Dedekind domain, decryption, encryption.

1. Introduction

In this paper we consider the structure of Dedekind in freely developed cryptosystems. This is the motivation coming from the reviewer of the paper [8].

Dedekind domain are one of the most important rings in algebra. It has many valuable properties and has many uses. Primary examples are Z, $K[X]$ (K is a field), Gauss rings, Krull rings.

Lemma 1.1. *For an integral domain R that is not a field, all the following conditions are equivalent:*

(a) *R is an integrally closed, Noetherian domain, every nonzero maximal ideal is prime.*

(b) *Every nonzero proper ideal factors into primes.*

(c) *R is Noetherian, and the localization at each maximal ideal is a discrete valuation ring.*

(d) *Every nonzero fractional ideal of R is invertible.*

An integral domain R satisfying one of the equivalent conditions of the above Lemma is called Dedekind domain.

In section 2 we introduce a cryptosystem where the key is analog to the fractional ideal. In section 3 we have a cryptosystem where an alphabet is analog to the fractional ideal.

Sections 4 and 5 are complementary of [8]. We present the application of polynomial composites and monoid domains in cryptology in the form of certain cryptosystems.

2. A key that is a fractional ideal

Let $A = \{a_0,a_1,...,a_n\}$ be an alphabet such that $|A|$ be a prime number. Let $x \in \{2,3,...,|A|\}$ be the value of one of the letters of the alphabet, $k > 2$ be an key. Then

$$y = xk \pmod{|A|},$$

where y be the value of one of the letters of the alphabet be an encrypted letter.

Now, assume we have encrypted letter y. Then we get a decrypted letter x by a formula

$$x = (y + (k - d) \cdot |A|) \cdot k^{-1},$$

where d be the remainder of dividing y by k.

Proof.

$$x = \frac{y + (k - y \pmod k)|A|}{k} =$$
$$= \frac{xk \pmod{|A|} + ((k - (xk \pmod{|A|})) \pmod k)|A|}{k} = x$$

As proposed in [8] (Introduction of section 3), this cipher can be generalized to a complete algebraic structure. It is enough to adopt the infinite alphabet as in [8], x be transformed into the principal ideal (x), k be transformed into the principal ideal (k), y into the principal ideal (y). This way we get algebraic encryption where the key (k) be the fractional ideal in the Dedekind's ring, in this case Z.

3. The alphabet as a fractional ideal

Let A be a set of characters. Assume $|A|$ is equal to any prime number.

Secretly establish a second alphabet A^0 such that $A^0 \subset A$ with a prime length.

Let $m_1m_2m_3...m_n$ be a message, we want to encrypt.

A secret short alphabet A^0 divides a large public alphabet into zones. We skip the extra characters such that 0, 1. So we have a clean alphabet from

2. Let's move one over, so we have 1. Suppose $p = |A|$, $q = |A^0|$. We have $\lceil \frac{p}{q} \rceil$ zones. Zero zone, includes the alphabet from 1 to q. The first zone, i.e. the alphabet from $q + 1$ to $2q$ and so on. The last zone $(\lceil \frac{p}{q} \rceil - 1)$ includes the alphabet from $\lceil \frac{p}{q} \rceil q$ to p.

Let's extend the message values with random numbers informing us about a given zone of a given letter (this information denote by z_i):

$$z1m1z2m2...znmn$$

Denote by k the key. Multiply each value of the message (not the information about the zone) by k and use the modulo q.

Hence ciphertext is:

$$z1d1z2d2...zndn,$$

where $d_1d_2...d_n$ be a encrypted message.

Now let's decode the message.

$$z1d1z2d3\ ...zndn$$

by dividing it into blocks (each block contains a zone and a message).

Let's apply the formula:

$$m_i = \frac{d_i + (z_i + t_i \cdot k)|A|}{k},$$

where m_i is the decoded letter, d_i encrypted letter, z is a number satisfies a congruence $|A|^{-1}z_i \equiv d_i \pmod{k}$, k be the key, t be a zone.

Of course, this cryptosystem can also be easily generalized by turning individual elements into ideals.

4. Applications of polynomial composites in cryptology

In 1976 [3] authors considered the structures in the form $D + M$, where D is a domain and M is a maximal ideal of ring R, where $D \subset R$. In [6] we could prove that in composite in the form $D + XK[X]$, where D is a domain, K is a field with $D \subset K$, that $XK[X]$ is a maximal ideal of $K[X]$. Next, Costa, Mott and Zafrullah ([4], 1978) considered composites in the form $D+XD_S[X]$, where D is a domain and D_S is a localization of D relative to the multiplicative subset S. In 1988 [2] Anderson and Ryckaert studied classes groups $D+M$. Zafrullah in [12] continued research on structure $D+XD_S[X]$ but he showed that if D is a GCD-domain, then the behaviour of $D^{(S)} = \{a_0 + {}^{P}a_iX^i \mid a_0 \in D, a_i \in D_S\} = D + XD_S[X]$ depends upon the relationship between S and the prime ideals P od D such that D_P is a valuation domain (Theorem 1, [12]). Fontana and Kabbaj in 1990 ([5]) studied the Krull and valuative dimensions of composite $D+XD_S[X]$. In 1991 there was an article ([1]) that collected all previous composites and the authors began to create a theory about composites creating results. In this paper, the structures under consideration were officially called as composites. After this article, various minor results appeared. But the most important thing is that composites have been used in many theories as examples. The first ordered results The first ordered results can be found in Matysiak's papers. In [6], [7], [11] we can find studies of polynomial composites in terms of many basic algebraic properties. In [9]

we have relationships between polynomial copmposites and certain field extensions. In [10] we have a construction of polynomial coposite as a sum of a field and a maximal ideal.

Consider A and B as rings such that $A \subset B$. Put $T = A + XB[X]$. The structure defined in this way is called a composite. (The definition comes from [1]).

I generalized the concept of a composite in two different directions.

Consider $A_0,A_1,...,A_{n-1}$ and B be rings for any $n \geq 0$ such that $A_0 \subset A_1 \subset \cdots \subset A_{n-1} \subset B$. Put $T_n = A_0 + A_1X + \cdots + A_{n-1}X^{n-1} + X^nB[X]$.

And let other $A_0,A_1,...,A_{n-1}$ and B be rings for any $n \geq 0$ such that there exists $i \in \{0,1,...,n-1\}$, where $A_i \not\subset A_{i+1}$ and for every $j \in \{0,1,...,n-1\}$ we have $A_j \subset B$. Put $T'_n = A_0 + A_1X + \cdots + A_{n-1}X^{n-1} + X^nB[X]$.

Each such polynomial is the sum of the products of the variable and the coefficient. And what if subsequent coefficient sets are appropriate cryptographic systems? Instead of encrypting with one system, we can create one system composed of many systems. Such a cipher is very difficult to break. If the spy detects encryption systems (composite coefficients), then the problem will be to find the right sum and product of such systems.

Assume that we have two people: Alice und Bob. Alice wants to send a message to Bob. Alice has one composite and Bob has another one composite.

They can build such composite by various encryption systems (even known ones). Let see note Lemma:

Lemma 4.1. *Let* $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + \sum_{j=n}^{m} a_jX^j$, $g = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + \sum_{j=n}^{m} b_jX^j \in T_n^0$, *where* $a_i,b_i \in A_i$ *for* $i = 0,1,...,n-1$ *and* $a_j,b_j \in B$ *for* $j = n,n+1,...m$. *Then*

$$fg \in A_0 + XB[X].$$

Put A_i,B_j $(i,j = 0,1,...,n-1)$ be different encryption systems. Then we have f and g are composition of encryption systems. No consider B. To improve security, let's fix that deg$f = n - 1$, deg$g = n - k$, where $k \in \{2,...n-1\}$. And such f, g Alice and Bob agree before the message is sent.

Alice and Bob multiply these composites to form one. We have $fg = (A_0 + A_1X + ...A_kX^k)(B_0 + B_1X + \cdots + B_lX^l) = A_0B_0 + (A_0B_1 + A1B0)X + \cdots + AkBlXk+l.$

Note that the sum and product of the encryption systems must be defined in the formula above. Definitions we leave Alice and Bob. But in this section we can put $S_iS_j : x \to (x)_{Si}(x)_{Sj}$ and $S_i + S_j : x \to ((x)_{Si})_{Sj}$. We can define the product and the sum of cryptosystems completely differently.

So in the product we encrypt the letter as two letters, the first in the first system and the second in the second system. And in the sum we encrypt the letter using the first system and then the second system. Of course, we can define completely different, at our discretion.

Assume that degree of fg is m and text to encrypt consists of more letters then $m + 1$. Then we divide the text into blocks of length $m + 1$. We can assume that $fg(0)$ encrypts the first letter of each block. Expression at X of fg encrypts the second letter of each block, and expression at X^2 of fg encrypts the third letter and so on.

Now, let's see how to decrypt in this idea.

Assume that we have an encrypted message $M_0M_1...M_n$. If our key is degree m, then we divide message on $m + 1$ partition. And every partion divide to two. Every two letters are one letter of message.

Earlier we define $S_iS_j : x \to (x)_{Si}(x)_{Sj}$ and $S_i + S_j : x \to ((x)_{Si})_{Sj}$. Then decryption of two letters M_lM_{l+1} $(l = 0,2,4,...)$ are $M_lM_{l+1} =$

$(Ml)Si(Ml+1)Sj = Nl,l+1$ (one letter) and $Ml = ((Ml)Si)Sj = (Nl)ij$ (one letter).

The use of many cryptosystems in various configurations in a polynomial composite increases our security. The security here lies in the fact that the encrypted message is resistant to breaking under many cryptanalyst criteria.

It is very easy to decrypt the message when you know the key.

5. Applications of monoid domains in cryptology

Recall that if F be a field and M be a submonoid of Q+ then we can construct a monoid domain:

$$F[M] = F[X;M] = \{a_0X^{m0} + \cdots + a_nX^{mn} \mid a_i \in F, m_i \in M\}.$$

Any alphabet of characters creates a finite set. Most ciphers are based on finite sets. But we can have the idea of using the infinite alphabet A, although in reality they can be cyclical sets with an index that would mean a given cycle. For example, A_0 - 0, B_0 - 1, … , Z_0 - 25, A_1 - 0, B_1 - 1, … , where A_i=A, …, Z_i=Z for i = 0,1,…. We see that this is isomorphic to a monoid N0 non-negative integers by a formula

$$f: \mathrm{A} \to \mathrm{N}, f(m_i) = i.$$

Then we can use a monoid domain by a map ϕ: A → F[A], $\phi(m_0,m_1,\ldots,m_n) = a_0X^{m0} + \ldots a_nX^{mn}$.

We want to encrypt the message $m_0m_1m_2\ldots m_n$ (the letters transform to numbers by a function ϕ). We establish the secret key X. Let F be a field. We determine any coefficients from this field: a_0, a_1, …, a_n. Then the message $m_0m_1m_2\ldots m_n$ be transformed into a polynomial of the form:

$$a0Xm0 + a1Xm1 + \cdots + anXmn.$$

We compute for i = 0,1,…,n: $d_i = a_iX^{mi}$ (mod |A|) (|A| must be prime) and then we have a decrypt message $d_0d_1\ldots d_n$.

To decrypt it we need to use a formula (for i = 0,1,…,n):

$$m_i = \log_X \frac{d_i}{a_i} \pmod{|\mathbb{A}|}.$$

Proof.

$$\log_X \frac{a_iX^{m_i}}{a_i} = m_i \pmod{|\mathbb{A}|}.$$

References

[1] Anderson, D.D., Anderson, D.F., Zafrullah, M., *Rings between D[X] and K[X]*, Houston J. of Mathematics, **17** (1991), 109–129.

[2] Anderson, D.F., Ryckaert, A., *The class group of D + M*, J. Pure Appl. Algebra, **52** (1988), 199–212.

[3] Brewer, J., Rutter, E., *D + M construction with general overrings*, Mich. Math. J., **23** (1976), 33–42.

[4] Costa, D., Mott, J., Zafrullah, M., *The construction D + $XD_S[X]$*, J. Algebra, **153** (1978), 423–439.

[5] Fontana, M., Kabbaj, S., *On the Krull and valuative dimension of D + $XD_S[X]$ domains*, J. Pure Appl. Algebra, **63** (1990), 231–245.

[6] Matysiak, L , *On properties of composites and monoid domains*, Accepted for printing in Advances and Applications in Mathematical Sciences, http://lukmat.ukw.edu.pl/On%20properties%20of%20composites%20and%20monoid%20domains.pdf, (2021).

[7] Matysiak, L , *ACCP and atomic properties of composites and monoid domains*, Accepted for printing in Indian Journal of Mathematics, http://lukmat.ukw.edu.pl/ACCP%20and%20atomic%20properties%20of%20composites%20and%20monoid%20domains.pdf, (2020).

[8] Matysiak, L , *Generalized RSA cipher and Diffie-Hellman protocol*, J. Appl. Math.& Informatics Vol.39 (2021), No. 1 - 2, pp. 93 – 103

[9] Matysiak, L , *Polynomial composites and certain types of fields extensions*, arXiv: 2011.09904, (2021).

[10] Matysiak, L , *K + M constructions with general overrings and relationships with polynomial composites*, arXiv: 2011.12777, (2021).

[11] Matysiak, L , *On some properties of polynomial composites*, arXiv: 2104.09657, (2021).

[12] Zafrullah, M., *The D + $XD_S[X]$ construction from GCD-domains*, J. Pure Appl. Algebra, **50** (1988), 93–107.