Rational formal power series

Jānis Buls, Aigars Valainis
Department of Mathematics, University of Latvia, Jelgavas iela 3,
Rīga, LV-1004 Latvia, buls1950@gmail.com; AValainis@gmail.com

Abstract

We are following [1] and [5]. Nevertheless, we are interested only in the clarification of proofs.

Keywords

finite commutative rings, formal power series

1. Structure of finite commutative rings

Our object of interest is an associative-commutative ring with a multiplicative identity element. In this text, the term ring will mean exactly such a ring, i.e., an associative-commutative ring with a multiplicative identity element. We will denote rings R commutative group by $R^{\times}$. In this section, we will consider only finite rings and we are following [1].

1.1. Definition. *Subset H of ring R, is called a subring if*

- *H is a subgroup of the additive group,*
- *H is a subsemigroup of the multiplicative semigroup.*

1.2. Definition. *Subring $\mathcal{I}$ of ring R is called an ideal if*

$$R\mathcal{I} \subseteq \mathcal{I}.$$

1.3. Proposition. *If $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_n$ are ideals of ring R, then mapping*

$$\Phi : R \to R/\mathcal{I}_1 \times R/\mathcal{I}_2 \times \cdots \times R/\mathcal{I}_n : r \mapsto (r + \mathcal{I}_1, r + \mathcal{I}_2, \ldots, r + \mathcal{I}_n)$$

is a ring homomorphism.

□ We will use notation $[x]_j \leftrightharpoons x + \mathcal{I}_j$.
Let $x, y \in R$, then

$$\begin{aligned}
\Phi(x+y) &= ([x+y]_1, [x+y]_2, \ldots, [x+y]_n) \\
&= ([x]_1 + [y]_1, [x]_2 + [y]_2, \ldots, [x]_n + [y]_n) \\
&= ([x]_1, [x]_2, \ldots, [y]_n) + ([y_1], [y]_2, \ldots, [y]_n) \\
&= \Phi(x) + \Phi(y) \\
\Phi(1) &= ([1]_1, [1]_2, \ldots, [1]_n),
\end{aligned}$$

$$
\begin{aligned}
\Phi(xy) &= ([xy]_1, [xy]_2, \dots, [xy]_n) \\
&= ([x]_1[y]_1, [x]_2[y]_2, \dots, [x]_n[y]_n) \\
&= ([x]_1, [x]_2, \dots, [y]_n)([y_1], [y]_2, \dots, [y]_n) \\
&= \Phi(x)\Phi(y). \quad \blacksquare
\end{aligned}
$$

1.4. Definition. *$\{0\}$ and R are called trivial ideals of ring R.*

All other ideals of ring R are called nontrivial ideals. Ideal $\mathcal{I}$ are called proper ideal if $\mathcal{I} \neq R$.

Let $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_n$ be proper ideals of ring R.

1.5. Definition. *Proper ideals $\mathcal{I}_k$ un $\mathcal{I}_m$, $1 \leq k < m \leq n$, are called coprime if $\mathcal{I}_k + \mathcal{I}_m = R$.*

Here $\mathcal{I}_k + \mathcal{I}_m \leftrightharpoons \{a + b \,|\, a \in \mathcal{I}_k \ \wedge \ b \in \mathcal{I}_m\}$

1.6. Example. $\mathcal{I}_1 = \{0, 2, 4\}$, $\mathcal{I}_2 = \{0, 3\}$ *are coprime ideals of ring $\mathbb{Z}_6$.*

$$\mathcal{I}_1\mathbb{Z}_6 = \{0, 2, 4\}\{0, 1, 2, 3, 4, 5\} = \{0, 2, 4\}$$

$$
\begin{array}{ccc}
2 \cdot 3 = 6 \equiv 0 & 2 \cdot 4 = 8 \equiv 2 & 2 \cdot 5 = 10 \equiv 4 \\
4 \cdot 3 = 12 \equiv 0 & 4 \cdot 4 = 16 \equiv 4 & 4 \cdot 5 = 20 \equiv 2
\end{array}
$$

$$\mathcal{I}_2\mathbb{Z}_6 = \{0, 3\}\{0, 1, 2, 3, 4, 5\} = \{0, 3\}$$

$$
\begin{array}{ccc}
3 \cdot 3 = 9 \equiv 3 & 3 \cdot 4 = 12 \equiv 0 & 3 \cdot 5 = 15 \equiv 3
\end{array}
$$

$\mathcal{I}_1+\mathcal{I}_2 = \{0, 2, 4\}+\{0, 3\} = \{0+0, 0+3, 2+0, 2+3, 4+0, 4+3\} = \{0, 3, 2, 5, 4, 7 \equiv 1\} = \mathbb{Z}_6$

Notice that

$$\forall x \in \mathcal{I}_1 \forall y \in \mathcal{I}_2 \ xy = 0.$$

1.7. Proposition. *If $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_n$ are coprime ideals of ring R, then*

$$\bigcap_{k=1}^{n} \mathcal{I}_k = \prod_{k=1}^{n} \mathcal{I}_k$$

Notice that

$$\prod_{k=1}^{n} \mathcal{I}_k \leftrightharpoons \Big\{\sum_k x_{k1}x_{k2}\dots x_{kn} \,|\, \forall j \ x_{kj} \in \mathcal{I}_j\Big\}.$$

Here, $\sum_k x_{k1}x_{k2}\dots x_{kn}$ denotes all possible finite sums of such form. In sum $\sum_k x_k y_k$ there is a possibility for $x_1 = x_2$, but if so then $y_1 \neq y_2$.

$\square$ As $\mathcal{I}_1$ un $\mathcal{I}_2$ are ideals, then

$$\mathcal{I}_1 \cap \mathcal{I}_2 = \{h \in R \,|\, h \in \mathcal{I}_1 \ \wedge \ h \in \mathcal{I}_2\}$$

is a proper ideal since $0 \in \mathcal{I}_1 \cap \mathcal{I}_2$. Notice that

$$\prod_{k=1}^{2} \mathcal{I}_k = \mathcal{I}_1\mathcal{I}_2 = \Big\{\sum_k x_k y_k \,|\, x_k \in \mathcal{I}_1 \ \wedge \ y_k \in \mathcal{I}_2\Big\}.$$

Each member of sum $\sum_k x_k y_k$ belongs to ideal A $\mathcal{I}_1$ and also to $\mathcal{I}_2$, therefore $\sum_k x_k y_k \in \mathcal{I}_1 \cap \mathcal{I}_2$. Hence $\mathcal{I}_1\mathcal{I}_2 \subseteq \mathcal{I}_1 \cap \mathcal{I}_2$.

Let $a \in \mathcal{I}_1 \cap \mathcal{I}_2$. As $\mathcal{I}_1$ and $\mathcal{I}_2$ are coprime ideals, then there exist such $x \in \mathcal{I}_1$ and $y \in \mathcal{I}_2$, that $x + y = 1$. Therefore

$$a = a \cdot 1 = a(x + y) = ax + ay = xa + ay \in \mathcal{I}_1\mathcal{I}_2.$$

Hence $\mathcal{I}_1 \cap \mathcal{I}_2 = \mathcal{I}_1\mathcal{I}_2$.

Notice that $\prod\limits_{k=1}^{n} \mathcal{I}_k \leftrightharpoons \{\sum_k x_{k1}x_{k2}\dots x_{kn} \,|\, \forall j\ x_{kj} \in \mathcal{I}_j\}$. As the ring is commutative, it follows that each member of $\sum_k x_{k1}x_{k2}\dots x_{kn}$ is a member of an arbitrary ideal $\mathcal{I}_k, k \in \overline{1,n}$, therefore $\prod\limits_{k=1}^{n} \mathcal{I}_k \subseteq \bigcap\limits_{k=1}^{n} \mathcal{I}_k$.

Further proof is inductive, assuming that ideals $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_{m+1}$ are pairwise coprime.

$$\bigcap_{k=1}^{m+1} \mathcal{I}_k = \big(\bigcap_{k=1}^{m} \mathcal{I}_k\big) \cap \mathcal{I}_{m+1} = \big(\prod_{k=1}^{m} \mathcal{I}_k\big) \cap \mathcal{I}_{m+1}$$

As all the pairs $\mathcal{I}_{m+1}, \mathcal{I}_k, k \in \overline{1,m}$ are coprime ideals, then there exist such $a_k \in \mathcal{I}_k, b_k \in \mathcal{I}_{m+1}$, that $a_k + b_k = 1$. Therefore

$$1 = (a_1 + b_1)(a_2 + b_2)\cdots(a_m + b_m) = a_1a_2\cdots a_m + B,$$

where B is a sum. Here each member of B contains some b_k as a multiplier, therefore $B \in \mathcal{I}_{m+1}$.

Let $a \in \bigcap\limits_{k=1}^{m+1} \mathcal{I}_k$, then

$$a = a \cdot 1 = a(a_1 + b_1)(a_2 + b_2)\cdots(a_m + b_m) = a_1a_2\cdots a_m a + aB$$

As $a \in \bigcap\limits_{k=1}^{m+1} \mathcal{I}_k$, it follows that $a \in \bigcap\limits_{k=1}^{m} \mathcal{I}_k$.

From the inductive assumption $\bigcap\limits_{k=1}^{m} \mathcal{I}_k = \prod\limits_{k=1}^{m} \mathcal{I}_k$. Therefore a can be written as a sum $\sum_k x_{k1}x_{k2}\dots x_{km}$, where $\forall x_{kj} \in \mathcal{I}_j$. Thus

$$aB = \sum_k x_{k1}x_{k2}\dots x_{km}B \in \prod_{k=1}^{m+1} \mathcal{I}_k,$$

and therefore

$$\begin{aligned} a &= a_1a_2\cdots a_m a + aB \\ &= a_1a_2\cdots a_m a + \sum_k x_{k1}x_{k2}\dots x_{km}B \in \prod_{k=1}^{m+1} \mathcal{I}_k. \quad \blacksquare \end{aligned}$$

1.8. Proposition. *If $\mathcal{I}, \mathcal{J}$ are coprime ideals, then $\mathcal{I}^m, \mathcal{J}^m$ also are coprime for all $m \in \mathbb{Z}_+$.*

Notice that $\mathcal{I}^m = \underbrace{\mathcal{I}\mathcal{I}\cdots\mathcal{I}}_{m}$.

$\square$ As $\mathcal{I}, \mathcal{J}$ are coprime ideals, then there exist such $a \in \mathcal{I}, b \in \mathcal{J}$, that $a + b = 1$. Hence

$$1 = (a + b)^2 = a^2 + 2ab + b^2.$$

- If $ab = 0$, then $a^2 + b^2 \in \mathcal{I}^2 + \mathcal{J}^2$;
- If $ab \neq 0$, then $2ab = 1 \cdot 2ab = 2(a+b)ab = 2a^2b + 2ab^2 \in \mathcal{I}^2 + \mathcal{J}^2$.

Further proof is inductive. If $\mathcal{I}^k, \mathcal{J}^k$ are coprime ideals, then there exist such $a \in \mathcal{I}^k, b \in \mathcal{J}^k$, that $a + b = 1$. Hence

$$1 = (a+b)^2 = a^2 + 2ab + b^2.$$

- If $ab = 0$, then $a^2 + b^2 \in \mathcal{I}^{k+1} + \mathcal{J}^{k+1}$;
- If $ab \neq 0$, then $2ab = 1 \cdot 2ab = 2(a+b)ab = 2a^2b + 2ab^2 \in \mathcal{I}^{k+1} + \mathcal{J}^{k+1}$.

We are using the property of ideals: if $a \in \mathcal{I}^{m+1}$, then $a \in \mathcal{I}^m$. This arises from

$$a = \sum_i x_{i1}x_{i2}x_{i3} \dots x_{im+1} = \sum_i (x_{i1}x_{i2})x_{i3} \dots x_{im+1} \in \mathcal{I}^m,$$

because $x_{i1}x_{i2} \in \mathcal{I}$. By further use of induction, it's provable that: if $a \in \mathcal{I}^{m+n}$, then $a \in \mathcal{I}^m$. ■

1.9. Proposition. *Ring homomorphism $f : G \to G'$ is monomorphism if and only if* Ker$f = 0$.

□ $\Rightarrow$ If $f(x) = 0$ and $x \neq 0$, then $f(0) = 0 = f(x)$. Therefore f is not an injection.

$\Leftarrow$ Let $f(x) = f(y)$, then $f(x-y) = 0$. As Ker$f = 0$, then $x - y = 0$, i.e., $x = y$. ■

1.10. Proposition. *Assume that $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_n$ are ideals of ring R. Mapping*

$$\Phi : R \to R/\mathcal{I}_1 \times R/\mathcal{I}_2 \times \dots \times R/\mathcal{I}_n : r \mapsto (r + \mathcal{I}_1, r + \mathcal{I}_2, \dots, r + \mathcal{I}_n)$$

is ring monomorphism if and only if $\bigcap\limits_{k=1}^{n} \mathcal{I}_k = 0$.

□ Let $\Phi(r) = ([0]_1, [0]_2, \dots, [0]_n)$. Therefore $r \in \bigcap\limits_{k=1}^{n} \mathcal{I}_k$. It shows that Ker$\Phi = \bigcap\limits_{k=1}^{n} \mathcal{I}_k$. From previous proposition follows that Φ is injective only when Ker$\Phi = 0$, i.e., $0 = \text{Ker}\Phi = \bigcap\limits_{k=1}^{n} \mathcal{I}_k$. ■

1.11. Lemma. *If $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_n$ are coprime ideals of ring R, then $\mathcal{I}_1$ and $\prod\limits_{k=2}^{n} \mathcal{I}_k$ are coprime ideals of ring R.*

□ We have (1.7. Proposition) $\prod\limits_{k=2}^{n} \mathcal{I}_k = \bigcap\limits_{k=2}^{n} \mathcal{I}_k$, therefore $\prod\limits_{k=2}^{n} \mathcal{I}_k$ is an ideal. As all pairs $\mathcal{I}_1, \mathcal{I}_k, k \in \overline{2,n}$ are coprime, then there exist such $a_k \in \mathcal{I}_1, b_k \in \mathcal{I}_k$, that $a_k + b_k = 1$. Hence

$$1 = (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n) = A + b_2b_3 \cdots b_n,$$

where A is a sum. Here each term of sum A contains some a_k as a multipler, therefore $A \in \mathcal{I}_1$.

Thus $1 = A + b_2b_3 \cdots b_n$, where $A \in \mathcal{I}_1$ and $b_2b_3 \cdots b_n \in \prod\limits_{k=2}^{n} \mathcal{I}_k$. ■

1.12. Proposition. *Assume that $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_n$ are ideals of ring R. Mapping*

$$\Phi : R \to R/\mathcal{I}_1 \times R/\mathcal{I}_2 \times \cdots \times R/\mathcal{I}_n : r \mapsto (r + \mathcal{I}_1, r + \mathcal{I}_2, \ldots, r + \mathcal{I}_n)$$

is a ring epimorphism if and only if for all different indexes $k, j \in \overline{1,n}$ ideals $\mathcal{I}_k, \mathcal{I}_j$ are coprime.

$\square$ $\Rightarrow$ If Φ is a epimorphism, then there exists such $x \in R$, that

$$\begin{aligned} \Phi(x) &= ([1]_1, [0]_2, \ldots, [0]_n). \\ \Phi(1-x) &= \Phi(1) - \Phi(x) \\ &= ([1]_1, [1]_2, \ldots, [1]_n) - ([1]_1, [0]_2, \ldots, [0]_n) \\ &= ([0]_1, [1]_2, \ldots, [1]_n) \end{aligned}$$

It shows that $1 - x \in \mathcal{I}_1$, and also $x \in \mathcal{I}_k$ for all $k \in \overline{2,n}$. Hence $1 \in \mathcal{I}_1 + \mathcal{I}_k$ for all $k \in \overline{2,n}$.

Generally, $m \in \overline{1,n}$ reasoning is similar. If Φ is an epimorphism, then there exist such $x_m \in R$, that $\Phi(x_m) = ([x_{m1}]_1, [x_{m2}]_2, \ldots, [x_{mn}]_n)$, where

$$x_{mj} = \begin{cases} 0, & \text{if } j \neq m; \\ 1, & \text{if } j = m. \end{cases}$$

$\Phi(1 - x_m) = ([y_{m1}]_1, [y_{m2}]_2, \ldots, [y_{mn}]_n)$, where

$$y_{mj} = \begin{cases} 1, & \text{if } j \neq m; \\ 0, & \text{if } j = m. \end{cases}$$

It shows that $1 - x_m \in \mathcal{I}_m$. Also $x_m \in \mathcal{I}_k$ for all $k \neq m$. Hence $1 \in \mathcal{I}_m + \mathcal{I}_k$ for all $k \neq m$.

$\Leftarrow$ Assume that all pairs $\mathcal{I}_k, \mathcal{I}_j$ of ideals are coprime.

If $n = 2$, then there exist such $x \in \mathcal{I}_1, y \in \mathcal{I}_2$, that $x + y = 1$. As $x = 1 - y$ and $y = 1 - x$, then

$$\begin{aligned} [x]_2 &= [1-y]_2 = [1]_2 - [y]_2 = [1]_2 - [0] = [1]_2, \\ [y]_1 &= [1-x]_1 = [1]_1 - [x]_1 = [1]_1, \\ \Phi(x) &= ([x]_1, [x]_2) = ([0]_1, [1]_2), \\ \Phi(y) &= ([y]_1, [y]_2) = ([1]_1, [0]_2), \\ \Phi(bx + ay) &= \Phi(b)\Phi(x) + \Phi(a)\Phi(y) \\ &= ([b]_1, [b_2])([0]_1, [1]_2) + ([a]_1, [a]_2)([1]_1, [0]_2) \\ &= ([0]_1, [b]_2) + ([a]_1, [0]_2) = ([a]_1, [b]_2). \end{aligned}$$

Hence mapping Φ is surjective. Further proof is inductive.

From (1.14. Lemma) follows, that $\mathcal{I}_1, \mathcal{I}_2\mathcal{I}_3 \cdots \mathcal{I}_n$ are coprime, therefore homomorphism

$$\Psi : R \to R/\mathcal{I}_1 \times R/\mathcal{I}_2\mathcal{I}_3 \cdots \mathcal{I}_n : r \mapsto (r + \mathcal{I}_1, r + \mathcal{I}_2\mathcal{I}_3 \cdots \mathcal{I}_n)$$

is surjective. From the inductions assumption, it follows that mapping

$$\Phi_2 : R \to R/\mathcal{I}_2 \times R/\mathcal{I}_3 \times \cdots R/\mathcal{I}_n : r \mapsto (r + \mathcal{I}_2, r + \mathcal{I}_3, \ldots, r + \mathcal{I}_n)$$

ir surjective. From the homomorphism theorem, there exists such homomorphism Φ_2^*, that diagram

$$\begin{tikzcd}
R \arrow[rr, "\Phi_2"] \arrow[dr, "\pi"'] & & R/\mathcal{I}_2 \times R/\mathcal{I}_3 \times \cdots \times R/\mathcal{I}_n \\
& R/\mathrm{Ker}\Phi_2 \arrow[ur, "\Phi_2^*"'] &
\end{tikzcd} \qquad (D)$$

is commutative. Additionally, homomorphism Φ_2^* is a monomorphism. Therefore $R/\mathrm{Ker}\Phi_2$ is isomorphic with ring $R/\mathcal{I}_2 \times R/\mathcal{I}_3 \times \cdots \times R/\mathcal{I}_n$ (homomorphism Φ_2 is also surjective).

From proof of (1.10. Proposition) follows, that $\mathrm{Ker}\Phi_2 = \bigcap\limits_{k=2}^{n} \mathcal{I}_k$, additionally (1.7. Proposition) $\bigcap\limits_{k=2}^{n} \mathcal{I}_k = \prod\limits_{k=2}^{n} \mathcal{I}_k$. Therefore

$$R/\mathcal{I}_2\mathcal{I}_3 \cdots \mathcal{I}_n \quad \text{isisomorphic with} \quad R/\mathcal{I}_2 \times R/\mathcal{I}_3 \times \cdots \times R/\mathcal{I}_n.$$

Hence mapping $\Phi_2^* : R/\mathcal{I}_2\mathcal{I}_3 \cdots \mathcal{I}_n \to R/\mathcal{I}_2 \times R/\mathcal{I}_3 \times \cdots \times R/\mathcal{I}_n$ is an isomorphism.

Let $([r_1]_1, [r_2]_2, \ldots, [r_n]_n) \in R/\mathcal{I}_1 \times R/\mathcal{I}_2 \times R/\mathcal{I}_3 \times \cdots \times R/\mathcal{I}_n$. Notice that

$$\begin{aligned}
\Phi_1 : r &\mapsto ([r]_1, [r]_2, \ldots, [r]_n), \\
\Phi_2 : r &\mapsto ([r]_2, [r]_3, \ldots, [r]_n).
\end{aligned}$$

From the inductions assumption, mapping Φ_2 is an epimorphism, therefore there exists such $x \in R$, that

$$\Phi_2 : x \mapsto ([r_2]_2, [r_3]_3, \ldots, [r_n]_n),$$

i.e., $[x]_2 = [r_2]_2, [x]_3 = [r_3]_3, \ldots, [x]_n = [r_n]_n$. Let's consider epimorphism

$$\Psi : r \mapsto (r + \mathcal{I}_1, r + \mathcal{I}_2\mathcal{I}_3 \ldots \mathcal{I}_n).$$

As mapping Ψ is an epimorphism, then there exists such $y \in R$, that

$$\Psi : y \mapsto (y + \mathcal{I}_1, y + \mathcal{I}_2\mathcal{I}_3 \ldots \mathcal{I}_n),$$

where $y + \mathcal{I}_1 = [y]_1 = [r_1]_1$ and $(\Phi_2^*)^{-1}([r_2]_2, [r_3]_3, \ldots, [r_n]_n) = y + \mathcal{I}_2\mathcal{I}_3 \ldots \mathcal{I}_n$. Notice that $[y]_1 = [r_1]_1$, thus

$$\Phi_1 : y \mapsto ([r_1]_1, [y]_2, [y]_3, \ldots, [y]_n).$$

Diagram (D) is commutative, therefore

$$\begin{aligned}
([y]_2, [y]_3, \ldots, [y]_n) &= \Phi_2(y) = \Phi_2^*(\pi(y)) = \Phi_2^*(y + \mathcal{I}_2\mathcal{I}_3 \ldots \mathcal{I}_n) \\
&= ([r_2]_2, [r_3]_3, \ldots, [r_n]_n).
\end{aligned}$$

Thus $\Phi_1 : y \mapsto ([r_1]_1, [r_2]_2, \ldots, [r_n]_n)$, showing that mapping Φ_1 is an epimorphism. ■

1.13. Definition. *Element e of ring R is called idempotent if $e^2 = e$. Idempotents e, f are called orthogonal if $ef = 0$.*

1.14. Definition. *Ideal $\mathcal{I}$ of ring R is called principal ideal, if there exist such $a \in R$, that $\mathcal{I} = aR$.*

1.15. Proposition. *The following statements are equivalent:*

1. *$R \cong R_1 \times R_2 \times \cdots \times R_n$; here all R_i are subrings of ring R;*
2. *There exist such orthogonal idempotents e_i, that $\sum\limits_{i=1}^{n} e_i = 1$ and $R_i \cong e_i R$;*
3. *$R \cong \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$, here all $\mathcal{I}_j$ are main ideals of ring R and $I_j \cong R_j$.*

$\square$ 1. $\Rightarrow$ 2. The unit element of ring $R_1 \times R_2 \times \cdots \times R_n$ is tuple $(1, 1, \ldots, 1)$. Therefore tuples $\delta_k = (\delta_{1k}, \delta_{2k}, \ldots, \delta_{nk})$ are idempotents of ring $R_1 \times R_2 \times \cdots \times R_n$. Here

$$\delta_{ik} = \begin{cases} 0, & \text{if } i \neq k; \\ 1, & \text{if } i = k. \end{cases}$$

Assume that $\varphi : R_1 \times R_2 \times \cdots \times R_n \to R$ is a ring isomorphism. Then $\varphi(\delta_k) \rightleftharpoons e_k$ is an idempotent of ring R, because

$$e_k = \varphi(\delta_k) = \varphi(\delta_k^2) = \varphi(\delta_k)\varphi(\delta_k) = e_k e_k = e_k^2,$$

additionally

$$1 = \varphi(1, 1, \ldots, 1) = \varphi(\sum_{k=1}^{n} \delta_k) = \sum_{k=1}^{n} \varphi(\delta_k) = \sum_{k=1}^{n} e_k.$$

$\varphi^{-1}(e_k e_i) = \varphi^{-1}(e_k)\varphi^{-1}(e_i) = (0, 0, \ldots, 0)$ if $i \neq k$. As φ is an isomorphism, then $e_k e_i = 0$ only if $i \neq k$. Let $x \in R$, then $\varphi^{-1}(x) = (x_1, x_2, \ldots, x_n)$, where all $x_j \in R_j$.

$$\begin{aligned} \varphi^{-1}(e_i x) &= \varphi^{-1}(e_i)\varphi^{-1}(x) \\ &= (0, 0, \ldots, \underbrace{1}_{i}, \ldots, 0)(x_1, x_2, \ldots, x_i, \ldots, x_n) \\ &= (0, 0, \ldots, x_i, \ldots, 0). \end{aligned}$$

Hence $e_i R \cong R_i$.

2. $\Rightarrow$ 3. $\mathcal{I}_j \leftrightharpoons e_j R$. Notice that $(e_1, e_2, \ldots, e_n)$ is the unit element of ring $\mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$. Let's prove that

$$\varphi : \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n \to R : (a_1, a_2, \ldots, a_n) \mapsto a_1 + a_2 + \cdots + a_n$$

is a ring isomorphism.

(i) Let $\bar{a} = (a_1, a_2, \ldots, a_n) \in \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$ and $\bar{b} = (b_1, b_2, \ldots, b_n) \in \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$, then

$$\begin{aligned} \varphi(\bar{a} + \bar{b}) &= \varphi(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \\ &= a_1 + b_1 + a_2 + b_2 + \cdots + a_n + b_n \\ &= (a_1 + a_2 + \cdots + a_n) + (b_1 + b_2 + \cdots + b_n) \\ &= \varphi(\bar{a}) + \varphi(\bar{b}). \end{aligned}$$

(ii) If $x \in \mathcal{I}_j, y \in \mathcal{I}_k$ and $j \neq k$, then $xy = 0$. As $x \in \mathcal{I}_j$, then there exist such $x' \in R$, that $x = e_j x'$. Also, there exists such $y' \in R$, that $y = e_k y'$. Hence $xy = e_j x' e_k y' = e_j e_k x' y' = 0 x' y' = 0$.

$$\begin{aligned}
\varphi(\bar{a}\bar{b}) &= \varphi((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)) \\
&= \varphi(a_1 b_1, a_2 b_2, \ldots, a_n b_n) \\
&= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \\
&= (a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) \\
&= \varphi(\bar{a})\varphi(\bar{b}).
\end{aligned}$$

(iii) Assume that $x \in \mathcal{I}_j \cap \mathcal{I}_k$, then $x \in \mathcal{I}_j = e_j R$ and $x \in \mathcal{I}_k = e_k R$. Therefore $x = e_j x_j = e_k x_k$, where x_j, x_k are elements of ring R.

If $j \neq k$, then $e_j e_k = 0$, hence

$$x = e_j x_j = e_j^2 x_j = e_j e_k x_k = 0 \cdot x_k = 0.$$

Thus $\mathcal{I}_j \cap \mathcal{I}_k = 0$.

Let $y \in \mathcal{I}_k = e_k R$. Then $y = e_k y_k$, where $y_k \in R$. If $i \neq k$, then $e_i y = e_i e_k y_k = 0 \cdot y_k = 0$.

(iv) Let $\varphi(\bar{a}) = \varphi(\bar{b})$, i.e.,

$$a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_n,$$

then

$$a_i - b_i = \sum_{j \neq i} (b_j - a_j). \tag{1}$$

As for all k a_k and b_k are elements of ideal $\mathcal{I}_k = e_k R$, then $a_k = e_k x_k, b_k = e_k y_k$, where x_k, y_k belongs to ring R. Expression (1) can be written as

$$\begin{aligned}
e_i(x_i - y_i) &= \sum_{j \neq i} e_j (y_j - x_j), \\
e_i(x_i - y_i) = e_i^2 (x_i - y_i) &= \sum_{j \neq i} e_i e_j (y_j - x_j) = 0.
\end{aligned}$$

Then $a_i - b_i = e_i x_i - e_i y_i = 0$ or $a_i = b_i$. We have proven that φ is injective.

(v) Let $x \in R$ and $x_k = e_k x$, then $\forall k$ $x_k \in e_k R = \mathcal{I}_k$ and

$$\begin{aligned}
(x_1, x_2, \ldots, x_n) &\in \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n, \\
x_1 + x_2 + \cdots + x_n &= e_1 x + e_2 x + \cdots + e_n x \\
&= (e_1 + e_2 + \cdots + e_n) x = 1 \cdot x = x.
\end{aligned}$$

Hence $\varphi(x_1, x_2, \ldots, x_n) = x$. Therefore φ is surjective. We can conclude that φ is an isomorphism, therefore $R \cong \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$.

3. $\Rightarrow$ 1. An ideal is a subring of a ring. ■

1.16. Definition. *Ideal $\mathcal{I}$ of commutative ring R is called a prime ideal if*

$$ab \in \mathcal{I} \Rightarrow a \in \mathcal{I} \ \vee \ b \in \mathcal{I}.$$

1.17. Definition. *Ideal $\mathcal{M}$ of ring $R, \mathcal{M} \neq R$ is called maximal ideal if for any ideal $\mathcal{I}$ of ring R:*

$$\mathcal{M} \subseteq \mathcal{I} \subseteq R \Rightarrow \mathcal{M} = \mathcal{I} \ \vee \ \mathcal{I} = R.$$

1.18. Lemma. *If $\mathcal{I}$ and $\mathcal{J}$ are ideals of commutatve ring R, then $\mathcal{I} + \mathcal{J}$ is ideal of ring R.*

$\square$ Let a, b be elements of ideal $\mathcal{I}$ and, in turn, x, y to be elements of ideal $\mathcal{J}$. Thus $a + x$ and $b + y$ are elements of set $\mathcal{I} + \mathcal{J}$.

(i) $(a + x) + (b + y) = (a + b) + (x + y) \in \mathcal{I} + \mathcal{J}$. $-a - b \in \mathcal{I} + \mathcal{J}$. $0 = 0 + 0 \in \mathcal{I} + \mathcal{J}$.

(ii) Let $r \in R$. Then $r(a + x) = ra + rb \in \mathcal{I} + \mathcal{J}$. Hence $\mathcal{I} + \mathcal{J}$ is an ideal. $\blacksquare$

Let's denote the equivalence class of element x in the quotient ring by $[x]$.

1.19. Proposition. *If $1 \in R$ and $\mathcal{M}$ is maximal ideal of commutative ring R, then quotient ring $R/\mathcal{M}$ is a field.*

$\square$ Assume that $[x] \neq [0]$, then $x \notin \mathcal{M}$. Thus $\mathcal{M} + Rx \neq \mathcal{M}$ and $\mathcal{M} + Rx = R$. Then exist such $x \in \mathcal{M}$ and $y \in R$, that $(u + yx = 1)$. Thus for equivalence classes: $[1] = [u + yx] = [u] + [yx] = [0] + [y][x] = [y][x]$. $\blacksquare$

1.20. Corollary. *If $\mathcal{M}$ is a maximal ideal of ring R, then $\mathcal{M}$ is a prime ideal.*

$\square$ $R/\mathcal{M}$ is a field. A field is a ring without zero divisors. $\blacksquare$

1.21. Proposition. *If $\mathcal{M}$ is ideal of commutative ring R and $R/\mathcal{M}$ is a field, then $\mathcal{M}$ is maximal ideal of ring R.*

$\square$ As $R/\mathcal{M}$ is a field, then $\mathrm{card}(R/\mathcal{M}) \geq 2$. Let $\mathcal{M} \neq R$. If $\mathcal{I}$ is an ideal such that $\mathcal{M} \subset \mathcal{I} \subseteq R$, then exists $x \in \mathcal{I}$, that $x \notin \mathcal{M}$. As $[x] \neq [0]$, then there exists such y, that $[xy] = [x][y] = [1]$. As $[xy] = xy + \mathcal{M}$, therefore exist such $u \in \mathcal{M}$, that $u + xy = 1$. We have $\mathcal{M} \subset \mathcal{I}$, therefore $u \in \mathcal{I}$, $xy \in \mathcal{I}y \subseteq \mathcal{I}$ because $\mathcal{I}$ is an ideal. Thus $1 = u + xy \in \mathcal{I}$. Hence $\mathcal{I} = R$. $\blacksquare$

1.22. Definition. *The set of all prime ideals of ring R is called the spectrum of ring R and is denoted by $Spec(R)$. The set of all maximal ideals of ring R is called the maximal spectrum of ring R and is denoted by $Specm(R)$.*

1.23. Corollary. *$Specm(R) \subseteq Spec(R)$.*

1.24. Definition. *Jacobson radical:*

$$\mathcal{J}(R) \leftharpoondown \bigcap_{\mathcal{I} \in Specm(R)} \mathcal{I}.$$

1.25. Theorem. *$\mathcal{I}$ is prime ideal of ring R if and only if $R/\mathcal{I}$ is an integral domain.*

□ An integral domain is a nonzero commutative ring with no nonzero zero divisors.

$\Rightarrow$ $[a][b] = [0]$ implies $ab \in \mathcal{I}$. If $\mathcal{I}$ is prime, then $a \in \mathcal{I} \vee b \in \mathcal{I}$. Thus $[a] = [0] \vee [b] = [0]$. Hence $R/\mathcal{I}$ is an integral domain.

$\Leftarrow$ Assume that $\mathcal{I}$ is not prime, then exist such $a \notin \mathcal{I}$ and $b \notin \mathcal{I}$, that $ab \in \mathcal{I}$. $[a][b] = [0] \in R/\mathcal{I}$ and $[a] \neq [0] \wedge [b] \neq [0]$. Hence $R/\mathcal{I}$ is not an integral domain. ■

1.26. Proposition. *A finite integral domain is a field.*

□ Let $R = \{a_1, a_2, \ldots, a_n\}$ be a finite integral domain, $a \in R$ and $a \neq 0$. Consider terms $aa_1, aa_2, \ldots, aa_n$. All those terms are unique. If the contrary is true, then $aa_i = aa_j$. Thus $aa_i - aa_j = 0$, $a(a_i - a_j) = 0$. As R is an integral domain and $a \neq 0$, then $a_i - a_j = 0$, i.e., $a_i = a_j$. As

$$R = \{aa_1, aa_2, \ldots, aa_n\},$$

therefore there exists such a_k, that $aa_k = 1$. As an integral domain is commutative, then $1 = aa_k = a_k a$. Hence $a_k = a^{-1}$. ■

1.27. Corollary. *If $\mathcal{I}$ is a prime ideal of ring R, then it is a maximal ideal.*

□ As $\mathcal{I}$ is a prime ideal, then (1.25. Theorem) $R/\mathcal{I}$ is an integral domain. Integral domain $R/\mathcal{I}$ is finite, therefore (1.26. Proposition) it is a field. Thus (1.21. Proposition) ideal $\mathcal{I}$ is maximal. ■

1.28. Proposition. *If $\mathcal{I}$ and $\mathcal{J}$ are distinct maximal ideals of ring R, then they are coprime ideals.*

□ As $\mathcal{I} \neq \mathcal{J}$, then $\mathcal{I} + \mathcal{J} \supset \mathcal{I}$ or $\mathcal{I} + \mathcal{J} \supset \mathcal{J}$. Thus

$$R \supseteq \mathcal{I} + \mathcal{J} \supset \mathcal{I} \quad \text{or} \quad R \supseteq \mathcal{I} + \mathcal{J} \supset \mathcal{J}.$$

Notice that $\mathcal{I} + \mathcal{J}$ is ideal (1.18. Lemma) and $\mathcal{I}$, $\mathcal{J}$ are maximal ideals. Its possible only if $\mathcal{I} + \mathcal{J} = R$. ■

1.29. Definition. *Element $a \in R$ is called a nilpotent element, if exists such natural n, that $a^n = 0$.*

1.30. Definition. *Set $Nil(R)$, consisting of all nilpotent elements of ring R, is called a nilradical.*

1.31. Proposition. *$Nil(R)$ is ideal of ring R.*

□ Assume that $a^n = 0 = b^m$, then

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}.$$

While $k < n$, we have $n + m - k > m$. As a result, all terms of sum are equal to 0.

Let $r \in R$, then $(ra)^n = r^n a^n = r^n \cdot 0 = 0$. Thus $RNil(R) \subseteq Nil(R)$. ■

1.32. Proposition. *If R is a commutative ring, then*

$$Nil(R) = \bigcap_{\mathcal{I} \in Spec(R)} \mathcal{I}.$$

$\square$ Let $r \in Nil(R)$, Then there exists such n, that $r^n = 0 \in \mathcal{I} \in Spec(R)$. $\mathcal{I}$ is an ideal, therefore $0 \in \mathcal{I}$. $\mathcal{I}$ is prime ideal and $r \cdot r^{n-1} \in \mathcal{I}$, therefore $r \in \mathcal{I}$ or $r^{n-1} \in \mathcal{I}$. If $r \in \mathcal{I}$, then we have obtained the desired result. If the contrary is true, then we proceed inductively, i.e., we assume that $r^{n-k} \in \mathcal{I}$ and $n-k > 1$, then $r \cdot r^{n-k-1} \in \mathcal{I}$ and therefore $r \in \mathcal{I}$ or $r^{n-k-1} \in \mathcal{I}$. We proceed until $n-k-i = 1$. Thus we have proven, that $r \in \mathcal{I}$ for any $\mathcal{I} \in Spec(R)$. Thus $r \in \cap_{\mathcal{I} \in Spec(R)} \mathcal{I}$ and $Nil(R) \subseteq \cap_{\mathcal{I} \in Spec(R)} \mathcal{I}$.

Let's now assume that $f \notin Nil(R)$ and consider set

$$\mathfrak{F} \leftharpoondown \{J \subseteq R \,|\, J \text{ is an ideal and } \forall m \in \mathbb{Z}_+ \; f^m \notin J\}.$$

Set $\mathfrak{F} \neq \emptyset$, because 0 is an ideal. Set $\mathfrak{F}$ is partially ordered with respect to $\subseteq$, and for each chain $J_1 \subseteq J_2 \subseteq \ldots$ there exist a upper bound

$$\mathfrak{J} \leftharpoondown \bigcup_{k>0} J_k.$$

Let's prove that $\mathfrak{J}$ is an ideal.

$\triangleright$ If $a \in \mathfrak{J}$ and $b \in \mathfrak{J}$, then $\exists i \; a \in J_i$ and $\exists k \; b \in J_k$. Assume for concreteness that $J_i \subseteq J_k$, then $a \in J_k$. Hence $a + b \in J_k \subseteq \mathfrak{J}$.

Let $r \in R$ un $c \in \mathfrak{J}$, then $\exists \varkappa \; c \in J_\varkappa$. Hence $rc \in J_\varkappa \subseteq \mathfrak{J}$. $\triangleleft$

Let $f^m \in \mathfrak{J}$, then $\exists k \; f^m \in J_k$. A contradiction!

As for each such chain an upper bound exists, then by Zorn's lemma, in set $\mathfrak{F}$ exists a maximal element $\mathcal{M}$. Let's prove that $\mathcal{M} \in Spec(R)$.

$\triangleright$ Let $a \notin \mathcal{M}$ and $b \notin \mathcal{M}$, then $aR + \mathcal{M} \supset \mathcal{M}$ and $bR + \mathcal{M} \supset \mathcal{M}$. Therefore $aR + \mathcal{M} \notin \mathfrak{F}$ and $bR + \mathcal{M} \notin \mathfrak{F}$, thus

$$\exists n \; f^n \in aR + \mathcal{M} \quad \text{and} \quad \exists m \; f^m \in bR + \mathcal{M}.$$

As $f^n \in aR + \mathcal{M}$, then $f^n = ar_1 + m_1$, where $r_1 \in R$ and $m_1 \in \mathcal{M}$. Similarly $f^m \in bR + \mathcal{M}$, $f^m = br_2 + m_2$, where $r_2 \in R$ and $m_2 \in \mathcal{M}$.

$$f^{n+m} = f^n f^m = (ar_1 + m_1)(br_2 + m_2) = abr_1r_2 + ar_1m_2 + br_2m_1 + m_1m_2.$$

Hence $f^{m+n} \in abR + \mathcal{M}$. Therefore $abR + \mathcal{M} \notin \mathfrak{F}$, thus $ab \notin \mathcal{M}$.

With some logical transformations:

$$\begin{array}{rcl}
a \notin \mathcal{M} \wedge b \notin \mathcal{M} & \Rightarrow & ab \notin \mathcal{M}, \\
\neg(a \notin \mathcal{M} \wedge b \notin \mathcal{M}) & \vee & ab \notin \mathcal{M}, \\
a \in \mathcal{M} \vee b \in \mathcal{M} & \vee & ab \notin \mathcal{M}, \\
ab \notin \mathcal{M} & \vee & a \in \mathcal{M} \vee b \in \mathcal{M}, \\
ab \in \mathcal{M} & \Rightarrow & a \in \mathcal{M} \vee b \in \mathcal{M}.
\end{array}$$

Therefore $\mathcal{M}$ is a prime ideal. $\triangleleft$

Thus if element f is not nilpotent, then there exists such prime ideal $\mathcal{M}$ to whom f doesn't belong.

$$f \notin Nil(R) \Rightarrow \exists \mathcal{M} \in Spec(R) \; (f \notin \mathcal{M}).$$

From contraposition, we obtain:

$$\forall \mathcal{M} \in Spec(R)\ (f \in \mathcal{M}) \Rightarrow f \in Nil(R).$$

Thats proves the inclusion $\bigcap\limits_{\mathcal{I} \in Spec(R)} \mathcal{I} \subseteq Nil(R)$. ■

1.33. Lemma. *There exists m, that $(Nil(R))^m = 0$.*

□ If $a \in Nil(R)$, then there exists such κ_a, that $a^{\kappa_a} = 0$. As R is a finite set, then $Nil(R)$ also is a finite set, therefore there exists

$$\kappa \leftharpoondown\!\!= \max_{a \in Nil(R)} (\kappa_a).$$

Let's assume for concreteness, that $|Nil(R)| = n$. In product $a_1 a_2 \dots a_m$, where all $a_i \in Nil(R)$ and $m = n\kappa$, there is at least one nilpotent element a_j, whose power ν is no less than κ, i.e., $\nu \geq \kappa$, therefore $a_j^\nu = 0$. ■

1.34. Lemma. *If $\phi : R \to R'$ is a ring epimorphism and $\mathcal{I}$ is a ideal of ring R, then $\phi(\mathcal{I})$ is ideal of R'.*

□ (i) Let $x' \in R'$ and $a' \in \phi(\mathcal{I})$, then there exist such $x \in R$ and $a \in \mathcal{I}$, that $\phi(x) = x'$ and $\phi(a) = a'$. As $x \in R$ and $a \in \mathcal{I}$, then $ax \in \mathcal{I}$, therefore

$$a'x' = \phi(a)\phi(x) = \phi(ax) \in \phi(\mathcal{I}).$$

(ii) Notice that $\phi : \mathcal{I} \to R'$ is a ring homomorphism, then according to the theorem of homomorphism $\phi(\mathcal{I})$ is a ring. ■

1.35. Lemma. *If $\phi : R \to R'$ is a ring epimorphism and $\mathcal{I}'$ is ideal of ring R', then there exists such $\mathcal{I}$ ideal of ring R, that $\phi(\mathcal{I}) = \mathcal{I}'$.*

□ (i) Let's define

$$\mathcal{I} \leftharpoondown\!\!= \{x \in G \,|\, \exists x' \in \mathcal{I}'\ \phi(x) = x'\}.$$

(ii) Let $a \in \mathcal{I}$ un $b \in \mathcal{I}$, then

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \in \mathcal{I}', \\ \phi(ab) &= \phi(a)\phi(b) \in \mathcal{I}'. \end{aligned}$$

Thus $a + b$ and ab belong to set $\mathcal{I}$.

(iii) Let $r \in R$, then $\phi(ra) = \phi(r)\phi(a) \in \mathcal{I}'$, because $\mathcal{I}'$ is a ideal of ring R'. Hence $ra \in \mathcal{I}$. ■

Let us consider groups. A subgroup, as usual, is denoted by $\leq$, and a normal subgroup is denoted by $\trianglelefteq$.

1.36. Lemma. *Let $N \trianglelefteq G$. If $K \leq G/N$, then there exists such $H \leq G$, that $K = H/N$.*

□ From the definition of K:

$$K = \{hN \,|\, hN \in K \,\wedge\, h \in G\}.$$

Let's define $H \leftharpoondown\!\!= \{h \,|\, hN \in \mathscr{H} \,\wedge\, h \in G\}$. Thus $h \in H \Leftrightarrow hN \in \mathscr{H}$. If $n \in N$, then $nN = N \in K$, because N is the unit element of group G/N.

(i) Assume that $g \in H$ and $h \in H$. As $K \leq G/N$, then

$$ghN = (gN)(hN) \in K.$$

Hence $gh \in H$.

(ii) As $hN \in K$, then $h^{-1}N = (hN)^{-1} \in K$. Thus accordingly to definition of H we have $h^{-1} \in H$. Thus $H \leq G$.

(iii) Notice

$$H/N = \{hN \mid h \in H\} = \{hN \mid hN \in K\} = K. \quad \blacksquare$$

1.37. Theorem (Correspondence theorem). *Let $N \trianglelefteq G$.*
(i) *If $N \subseteq H \trianglelefteq G$, then $H/N \trianglelefteq G/N$.*
(ii) *If $K \trianglelefteq G/N$, then there exist such $H \trianglelefteq G$, that $K = H/N$.*
(iii) *Let*

- $S = \{H \mid N \subseteq H \wedge H \trianglelefteq G\}$,
- $\mathscr{S} = \{K \mid K \trianglelefteq G/N\}$.

If $\phi : S \to G/N : H \mapsto H/N$, then $\phi : S \to \mathscr{S}$ is a bijection.

□ (i) Let $gN \in G/N$ un $hN \in H/N$, then

$$(gN)(hN)(gN)^{-1} = (ghN)(g^{-1}N) = ghg^{-1}N.$$

As $H \trianglelefteq G$, then $ghg^{-1} \in H$. Hence $ghg^{-1}N \in H/N$. Thus for each $gN \in G/N$ and any $hN \in H/N$ we have proven

$$(gN)(hN)(gN)^{-1} \in H/N.$$

Thus by definition $H/N \trianglelefteq G/N$.

(ii) There exists (1.36. Lemma) such $H \leq G$, that $K = H/N$. We need to prove that $H \trianglelefteq G$ and thus $H/N \trianglelefteq G/N$.

Let $g \in G$ and $h \in H$, then gN and $g^{-1}N$ belong to group G/N. In turn, hN belongs to group H/N. As $H/N \trianglelefteq G/N$, then

$$ghg^{-1}N = (gN)(hN)(gN)^{-1}N \in H/N.$$

Hence $ghg^{-1} \in H$. Thus for each $g \in G$ and any $h \in H$ we have proven, that $ghg^{-1} \in H$. Then according to the definition $H \trianglelefteq G$.

(iii) From (ii) for each element K of set $\mathscr{S}$ there exists such $H \trianglelefteq G$, that $K = H/N$. Thus range of $\phi : S \to G/N : H \mapsto H/N$ is $\mathrm{Ran}(\phi) = \mathscr{S}$, and thus mapping $\phi : S \to \mathscr{S}$ is surjective (with $\mathscr{S}$ as a codomain).

Assume that $\phi(H_1) = \phi(H_2)$, i.e., $H_1/N = H_2/N$. Let $h_1 \in H_1$, then $h_1N \in H_1/N = H_2/N$. Hence $h_1 \in H_2$. Thus $H_1 \subseteq H_2$. We may construct a symmetrical argument: $h_2 \in H_2$, then $h_2N \in H_2/N = H_1/N$ and $h_2 \in H_1$. Thus $H_2 \subseteq H_1$. Thus $H_1 \subseteq H_2 \subseteq H_1$, i.e., $H_1 = H_2$. We have proven that $\phi : S \to \mathscr{S}$ is an injection. ■

The correspondence theorem holds also for rings. We will consider commutative rings.

1.38. Theorem (Correspondence theorem for rings). *Assume that*

- *R is a ring;*
- *$\mathcal{I} \subseteq R$ is an ideal;*

- $\pi : R \to R/\mathcal{I} : r \mapsto [r]$ *is the natural mapping;*
- $S = \{G \,|\, \mathcal{I} \subseteq G$ and G is a subring of $R\}$*;*
- $\mathscr{S} = \{H \,|\, H$ ir a subring of ring $R/\mathcal{I}\ \}$.

Mapping $\phi : S \to \mathscr{S} : G \mapsto G/\mathcal{I}$ *is a bijction. If*

- $S' = \{\mathcal{J} \,|\, \mathcal{I} \subseteq \mathcal{J}$ and $\mathcal{J}$ is an ideal of $R\}$,
- $\mathscr{S}' = \{L \,|\, L$ is an ideal of ring $R/\mathcal{I}\}$,

then mapping $\psi : S' \to \mathscr{S}' : \mathcal{J} \mapsto \mathcal{J}/\mathcal{I}$ *is a bijection.*

□ (i) First we have to prove that mapping $\phi : S \to \mathscr{S} : G \mapsto G/\mathcal{I}$ is correctly defined,i.e., Ran$(\phi) \subseteq \mathscr{S}$. Assume that $\mathcal{I} \subseteq G$ is a subring of ring$R$. The image of the additive group of ring G (1.37. Theorem) is $G/\mathcal{I}$.As $\mathcal{I}$ is an ideal, then $G/\mathcal{I}$ is a ring. Thus we have proven that Ran$(\phi) \subseteq \mathscr{S}$.

For different subrings of ring R additive groups are distinct. Thus (1.37. Theorem) mapping ϕ is injective.

Let H be a subring of ring $R/\mathcal{I}$, then for H the additive group can be expressed as (1.37. Theorem) $H = A/\mathcal{I}$, where A is a subgroup of the additive group of ring R. Thus $a \in A \Leftrightarrow a + \mathcal{I} \in A/\mathcal{I}$. As $H = A/\mathcal{I}$ is a subring, then $(a + \mathcal{I})(b + \mathcal{I}) = ab + \mathcal{I}$ for all $a \in A$, $b \in A$. Therefore $ab \in A$, i.e., A is subring of ring G. According to the definition of ϕ, we have $\phi(A) = A/\mathcal{I}$. Thus mapping ϕ is surjective.

(ii) Let L be an ideal of ring $R/\mathcal{I}$, than the additive group of L can be expressed (1.37. Theorem) as $L = A/\mathcal{I}$, where A is a subroup of the additive group of ring R. Thus $a \in A \Leftrightarrow a + \mathcal{I} \in A/\mathcal{I}$. As $L = A/\mathcal{I}$ is an ideal, then $ra + \mathcal{I} = (r + \mathcal{I})(a + \mathcal{I}) \in A/\mathcal{I}$ for all $r \in R$, $a \in A$. Therefore $ra \in A$, i.e., A is an ideal of ring G. According to the definition ψ we have $\psi(A) = A/\mathcal{I}$. Hence mapping ψ is surjective.

Let $\mathcal{J}$ be an ideal of ring R and $\mathcal{I} \subseteq \mathcal{J}$. If we consider the additive group of $\mathcal{J}$, then (1.37. Theorem) mapping $\psi : \mathcal{J} \mapsto \mathcal{J}/\mathcal{I}$ is injective.

We must prove that $\mathcal{J}/\mathcal{I}$ is an ideal. From the definition of $\mathcal{J}/\mathcal{I}$ fallows, that $a \in \mathcal{J} \Leftrightarrow a + \mathcal{I} \in \mathcal{J}/\mathcal{I}$. If $r \in R$, then $ar \in \mathcal{J}$, thus

$$(a + \mathcal{I})(r + \mathcal{I}) = ar + \mathcal{I} \in \mathcal{J}/\mathcal{I}.$$

Therefore $\mathcal{J}/\mathcal{I}$ is ideal of ring $R/\mathcal{I}$. Hence mapping ψ is also injective. ■

1.39. Corollary. *Assume that*

- R *is a ring;*
- $\mathcal{I} \subseteq R$ *is an ideal;*
- $\pi : R \to R/\mathcal{I} : r \mapsto [r]$ *is the natural mapping;*
- $S' = \{\mathcal{J} \,|\, \mathcal{I} \subseteq \mathcal{J}$ and $\mathcal{J}$ is an ideal of $R\}$*;*
- $\mathscr{S}' = \{L \,|\, L$ is an ideal of ring $R/\mathcal{I}\}$*;*
- $\psi : S' \to \mathscr{S}' : \mathcal{J} \mapsto \mathcal{J}/\mathcal{I}$.

$\mathcal{J}/\mathcal{I}$ *is a maximal ideal of ring* $R/\mathcal{I}$ *if and only if* $\mathcal{J}$ *is a maximal ideal of ring* R*, and* $\mathcal{J}$ *contains ideal* $\mathcal{I}$.

$\square$ Notice that mapping ψ is bijective.

$\Rightarrow$ Assume that L is a maximal ideal if ring $R/\mathcal{I}$. We already know that there exist an ideal $\mathcal{J}$ of ring $\mathcal{R}$, $\mathcal{I} \subseteq \mathcal{J}$, that $L = \mathcal{J}/\mathcal{I}$ and $\psi(\mathcal{J}) = \mathcal{J}/\mathcal{I}$. If in turn, $\mathcal{J}$ is not a maximal ideal, then there exists such ideal $\mathfrak{M}$ of ring R, that $\mathcal{J} \subset \mathfrak{M} \subset R$. Thus if $\mathcal{J} \subset \mathfrak{M}$, then $\mathcal{J}/\mathcal{I} \subseteq \mathfrak{M}/\mathcal{I}$. As ψ is bijective, then $\mathcal{J}/\mathcal{I} \neq \mathfrak{M}/\mathcal{I}$. Thus $\mathcal{J}/\mathcal{I} \subset \mathfrak{M}/\mathcal{I}$, e.i., $\mathcal{J}/\mathcal{I}$ is not a maximal ideal. A contradiction!

$\Leftarrow$ Assume that $\mathcal{J}$ is a maximal ideal of ring R, $\mathcal{I} \subseteq \mathcal{J}$. If in turn, $\mathcal{J}/\mathcal{I}$ is not a maximal ideal of ring $R/\mathcal{I}$, then there exists such ideal M of ring $R/\mathcal{I}$, that $\mathcal{J}/\mathcal{I} \subset M \subset R/\mathcal{I}$. As M is an ideal of ring $R/\mathcal{I}$, then there exist such ideal $\mathfrak{M}$ of ring R, $\mathcal{I} \subseteq \mathfrak{M}$, that $\mathfrak{M}/\mathcal{I} = M$. Thus $\mathcal{J}/\mathcal{I} \subset \mathfrak{M}/\mathcal{I}$. Notice that

$$\begin{aligned} a + \mathcal{J} \in \mathcal{J}/\mathcal{I} \quad &\Leftrightarrow \quad a \in \mathcal{J}, \\ b + \mathcal{I} \in \mathfrak{M}/\mathcal{I} \quad &\Leftrightarrow \quad b \in \mathfrak{M}. \end{aligned}$$

Hence $\mathcal{J} \subseteq \mathfrak{M}$. As ψ is bijective, then $\mathcal{J} \neq \mathfrak{M}$. Thus $\mathcal{J} \subset \mathfrak{M}$. As $\mathfrak{M}/\mathcal{I} \subset R/\mathcal{I}$, then thre exist such $r \in R$, that $r + \mathcal{I} \notin \mathfrak{M}/\mathcal{I}$. Therefore $r \notin \mathfrak{M}$. Thus $\mathcal{J}$ is not a maximal ideal. A contradiction! $\blacksquare$

1.40. Definition. *A ring with only one maximal ideal is called a local ring.*

The commutative group of ring R is denoted as $R^{\times}$, i.e., it is the set of all invertible elements in ring R.

1.41. Proposition. *If $\mathfrak{M} \neq R$ is an ideal of ring R and $R^{\times} = R \backslash \mathfrak{M}$, then R is a local ring and $\mathfrak{M}$ is the maximal ideal.*

$\square$ (i) Assume that $\mathcal{I} \subseteq R$ is ideal of ring R and $a \in \mathcal{I} \cap R^{\times}$. Then $a^{-1} \in R$. As $\mathcal{I}$ is an ideal, then $1 = aa^{-1} \in \mathcal{I}$.

(ii) Assume that $r \in R$ and $r1 \in \mathcal{I}$. Thus $\mathcal{I} = R$. Thus any ideal $\mathcal{J} \subset R$ doesn't contain elements of set $R^{\times}$.

(iii) As ideal $\mathfrak{M}$ contain all the nonreversible (in ring R) elements of set R, then $\mathcal{J} \subseteq \mathfrak{M}$. Thus $\mathfrak{M}$ is the one maximal ideal. $\blacksquare$

1.42. Proposition. *If $\mathfrak{M}$ is the maximal ideal of local ring R, then $\mathfrak{M} = R \setminus R^{\times}$.*

$\square$ Assume that $a \notin R^{\times}$.

(i) It is obvious that $a \in aR$ and aR is a commutative group. If $r \in R$ and $b \in aR$, then $b = a\beta$, where $\beta \in R$ and $br = a\beta r \in aR$. Hence aR is an ideal.

As $a \notin R^{\times}$, then in ring R dosnt exist a^{-1}, therefore $1 \notin aR$ and $aR \subset R$, i.e., aR is a proper ideal of ring R.

(ii) Let

$$S \leftharpoondown \{\mathcal{I} \,|\, aR \subseteq \mathcal{I} \subset R, \text{ where } \mathcal{I} \text{ is an ideal of ring } R\}.$$

Let $\{\mathcal{J}_\alpha\}$ be a chain of set S, i.e., if $\mathcal{J}_\beta \in \{\mathcal{J}_\alpha\}$ and $\mathcal{J}_\gamma \in \{\mathcal{J}_\alpha\}$, then $\mathcal{J}_\beta \subset \mathcal{J}_\gamma$ or $\mathcal{J}_\gamma \subset \mathcal{J}_\beta$.

If $\mathcal{J} \leftharpoondown \bigcup\limits_{\alpha} \mathcal{J}_\alpha$, then $\mathcal{J} \subset R$ because $1 \notin \mathcal{J}$.

Let $b \in \mathcal{J}$ and $c \in \mathcal{J}$. Then there exist such β and γ, that $b \in \mathcal{J}_\beta$ and $c \in \mathcal{J}_\gamma$. We have $\mathcal{J}_\beta \subset \mathcal{J}_\gamma$ or $\mathcal{J}_\gamma \subset \mathcal{J}_\beta$. For concreteness assume $\mathcal{J}_\beta \subset \mathcal{J}_\gamma$, then b and c are elements of ideal $\mathcal{J}_\gamma$. As $\mathcal{J}_\gamma$ is an ideal, then $b + c \in \mathcal{J}_\gamma$ also $0 \in \mathcal{J}_\gamma$ and $-b \in \mathcal{J}_\gamma$. As $\mathcal{J}_\gamma$ is an ideal, then $br \in \mathcal{J}_\gamma$ for all $r \in R$. Thus $b + c, 0, -b, br$ belong to set $\mathcal{J}$, because $\mathcal{J}_\beta \subset \mathcal{J}$. Additionally, the sum is associative and commutative, while the multiplication is associative ($\mathcal{J} \subset R$). Thus $\mathcal{J}$ is an ideal. Thus $\mathcal{J} \in S$ and is upper bound of chain $\{\mathcal{J}_\alpha\}$. According to Zorn's lemma, set S has at least one maximal element $\mathfrak{N}$.Thus $\mathfrak{N}$ is a maximal ideal and$\mathfrak{N} \neq \mathfrak{M}$, because $a \notin \mathfrak{M}$ and $a \in \mathfrak{N}$. This gives us a contradiction because R is a local ring. ■

1.43. Lemma. *In a local ring, there are only two idempotent elements: 0 and 1.*

□ Assume that $0 \neq e \neq 1$ is idempotent. Then $e(1-e) = e - e^2 = 0$, i.e., both elements are zero divisors, thus $e \notin R^\times$ and $1 - e \notin R^\times$. Thus both elements belong to the maximal ideal, but $1 = e + (1 - e)$, i.e., 1 belongs to the maximal ideal. A contradiction! ■

1.44. Lemma. *If $e \in R$ is idempotent, then eR is a ring with unit element e.*

□ From (proof of 1.42. Proposition) eR is an ideal. Let's show that e is the unit element. Assume that $x \in eR$, then $x = er$, where $r \in R$.

$$xe = ex = e^2 r = er = x. \qquad ■$$

1.45. Theorem. *Finite ring R is isomorph to the direct sum of local rings (with precision to term order in the sum).*

□ Let $Spec(R) = \{P_1, P_2, \ldots, P_n\}$. As R is a finite ring, P_i is a maximal ideal (1.27. Corollary). Thus $Spec(R) = Specm(R)$, because each maximal ideal is also a prime ideal (1.20. Corollary). Hence

$$Nil(R) = \bigcap_{P \in Spec(R)} P = \bigcap_{P \in Specm(R)} P = \mathcal{J}(R),$$

Additionaly, if $k \neq \varkappa$, then ideals P_k and $P_\varkappa$ are coprime (1.28. Proposition). Thus (1.7. Proposition)

$$\bigcap_{k=1}^{n} P_k = \prod_{k=1}^{n} P_k.$$

Also there (1.33. Lemma) exists such m, that $\mathcal{J}(R)^m = 0$.

If $x \in \prod_{j=1}^{n} P_j^m$, then $x = \sum_k x_{k1} x_{k2} \ldots x_{kn}$, where all $x_{kj} \in P_j^m$. Each $x_{kj} = \sum_i y_{ikj1} y_{ikj2} \ldots y_{ikjm}$, where all $y_{ikj\nu} \in P_j$. As a result, x is representable as a sum, whose terms are a product of nm elements. By taking into account the commutativity of multiplication, elements can be rearranged so that in product term first m elements belong to set P_1, then in turn m elements belonging to set P_2 m, etc., until the last m elements belonging to set P_n. Thus

$$\prod_{j=1}^{n} P_j^m = \big(\prod_{j=1}^{n} P_j\big)^m = \mathcal{J}(R)^m.$$

Note (1.8. Proposition), that P_i^m, P_j^m ere coprime if $i \neq j$, therefore (1.7. Proposition) $\bigcap_{j=1}^n P_j^m = \prod_{j=1}^n P_j^m$.

Let's define a homeomorphism of rings

$$\Phi : R \to R/P_1^m \times R/P_2^m \times \cdots \times R/P_n^m : r \mapsto ([r]_1, [r]_2, \ldots, [r]_n)$$

Homeomorphism Φ is injective (1.10. Proposition), because

$$\bigcap_{j=1}^n P_j^m = \prod_{j=1}^n P_j^m = (\prod_{j=1}^n P_j)^m = \mathcal{J}(R)^m = 0,$$

Additionally Φ is surjective (1.12. Proposition), because P_i^m, P_j^m are coprime, if $i \neq j$. Thus Φ is an isomorphism.

(i) We have a natural mapping

$$\Phi_i : R \to R/P_i^m : r \mapsto [r]_i.$$

Thus (1.38. Theorem) each ideal P (of ring R) containing P_i^m is mapped to ideal of ring R/P_i^m. Additionally mapping $\phi : P \mapsto P/P_i^m$ is bijective.

(ii) From (1.8. Proposition) we have: if $k \neq l$, then P_k^m, P_l^m are coprime, because P_k, P_l are coprime. Thus $P_k^m + P_l^m = R$. Assume that $P_k^m \subseteq P_l$, then $R = P_k^m + P_l^m \subseteq P_l + P_l^m \subseteq P_l + P_l = P_l$. A contradiction!

Hence P_k is the one maximal ideal, containing P_k^m. Thus from (1.39. Corollary): P_k/P_k^m is the one maximal ideal of ring R/P_k^m. Thus R/P_k^m is a local ring.

(iii) Assume that $R \cong \bigoplus_{j=1}^n R_j \cong \bigoplus_{k=1}^m S_k$, where all R_j, S_k are local rings. From (1.15. Proposition) there exist such orthogonal idempotents $e_j \in R, f_k \in R$, that $R_j \cong e_j R$, $S_k \cong f_k R$ and

$$1 = \sum_{j=1}^n e_j = \sum_{k=1}^m f_k.$$

Hence

$$\begin{aligned} e_j &= e_j \sum_{k=1}^m f_k = \sum_{k=1}^m e_j f_k \in e_j R, \\ (e_j f_k)^2 &= e_j^2 f_k^2 = e_j f_k. \end{aligned}$$

If $s \neq k$, then $(e_j f_k)(e_j f_s) = e_j^2 f_k f_s = e_j \cdot 0 = 0$. Thus

$$e_j f_1, e_j f_2, \ldots, e_j f_m$$

are orthogonal idempotents of ring $e_j R$. As $e_j R$ is a local ring, then

$$e_j f_k = 0, \quad \text{vai} \quad e_j f_k = e_j.$$

Note that (1.44. Lemma) e_j is unit element of ring $e_j R$. As all these idempotents $e_j f_1, e_j f_2, \ldots, e_j f_m$ are orthogonal, then only one of them is not equal to 0 (all can't be equal to 0, because $e_j = \sum_{k=1}^m e_j f_k$). Hence there exists such κ, that $e_j = e_j f_\kappa = f_\kappa e_j \in f_\kappa R$. As in the local ring $f_\kappa R$, exists only 2 idempotents, then $e_j = f_\kappa$. Thus

$$\{e_1, e_2, \ldots, e_n\} \subseteq \{f_1, f_2, \ldots, f_m\}.$$

Similarly, we can make an argument for

$$\{f_1, f_2, \ldots, f_m\} \subseteq \{e_1, e_2, \ldots, e_n\}.$$

Hence $n = m$ and

$$\{e_1, e_2, \ldots, e_n\} = \{f_1, f_2, \ldots, f_n\}. \quad \blacksquare$$

2. Periodical rings

We are following [5] in this section.

Assume $X \notin R$. We identify set R^ω with $R[[X]]$, i.e., by using standart notation

$$a_0 a_1 a_2 \cdots a_n \cdots \mapsto \sum_{k=0}^{\infty} a_k X^k.$$

If $f = \sum\limits_{k=0}^{\infty} a_k X^k$, then we use notation for coeficient extraction $f(n) = a_n$.

2.1. Definition. *Algebra $\langle R[[X]], +, \cdot \rangle$ is called formal power series if*

$$\begin{aligned} \sum_{k=0}^{\infty} a_k X^k + \sum_{k=0}^{\infty} b_k X^k &= \sum_{k=0}^{\infty} (a_k + b_k) X^k, \\ \left(\sum_{k=0}^{\infty} a_k X^k\right)\left(\sum_{k=0}^{\infty} b_k X^k\right) &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k. \end{aligned}$$

We use "formal power series" (or simply "series") also when referring to a concrete $f \in R[[X]]$.

2.2. Proposition. *Series $f = \sum\limits_{k=0}^{\infty} a_k X^k$ are invertible in algebra $R[[X]]$ if and only if $a_0 \in R^\times$.*

This is a standard result found in textbooks dedicated to formal power series. If series $A = a_0 + a_1 X + ...$ has a multiplicative inverse $B = b_0 + b_1 X + ...$, then the constant term $a_0 b_0$ of $A \cdot B$ is the constant term of the identity series, i.e., it is 1. The condition of invertibility of a_0 in R is also sufficient, coefficients of the inverse series B can be computed as:

$$b_0 = a_0^{-1}; \;\; b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-1}, \; n \geq 1.$$

Polynomial ring $R[X]$ is a subring of ring $R[[X]]$.

2.3. Definition. *Series $f \in R[[X]]$ is called rational series, if $f = \frac{h}{g}$, where $h, g \in R[X]$ and g is invertible in ring $R[[X]]$.*

2.4. Definition. *Series $f = \sum\limits_{i=0}^{\infty} a_i X^i$ is called periodical series if there exists such*

$$k \in \mathbb{Z}_+ = \{1, 2, \ldots, n, \ldots\},$$

that $\forall i \; a_i = a_{i+k}$. Series f is called semiperiodic series, if there exist such $n \in \mathbb{Z}_+$, that series $\sum\limits_{j=0}^{\infty} a_{j+n} X^j$ is periodical.

2.5. Proposition. *If series $f \in R[[X]]$ is semiperiodic series, then series f is rational series.*

$\square$ If $f = \sum\limits_{k=0}^{\infty} a_k X^k$, then there exist such m and n, that $\forall i > m \; a_i = a_{i+n}$. Hence

$$\begin{aligned} f &= a_0 + a_1 X + \ldots + a_m X^m \\ &+ \sum_{i=0}^{\infty} (a_{m+1} X^{m+1} + a_{m+2} X^{m+2} + \ldots + a_{m+n} X^{m+n}) X^{in} \\ &= p(X) + q(X) \sum_{i=0}^{\infty} X^{in} \\ &= p(X) + \frac{q(X)}{1 - X^n}. \end{aligned}$$

Here

$$\begin{aligned} p(X) &= a_0 + a_1 X + \ldots + a_m X^m, \\ q(X) &= a_{m+1} X^{m+1} + a_{m+2} X^{m+2} + \ldots + a_{m+n} X^{m+n}. \quad \blacksquare \end{aligned}$$

2.6. Definition. *Ring R is called a periodic ring, if*

$$\forall a \in R \; \exists m \in \mathbb{Z}_+ \; \exists n \in \mathbb{Z}_+ \; (m \neq n \; \wedge \; a^m = a^n).$$

2.7. Definition. *$n \in \mathbb{N}$ is called characteristic of ring R, denoted by* $\mathrm{char}(R)$*, if $\mathbb{Z}n$ is the kernel of homomorphism*

$$\lambda : \mathbb{Z} \to R : k \mapsto k1.$$

2.8. Corollary. *If R is a periodical ring, then* $\mathrm{char}(R) \neq 0$.

$\square$ Let e be the unit element of periodic ring R. If $e \neq 0$ and $e + e = 0$, then $\mathrm{char}(R) = 2$. Assume that $e \neq 0 \neq e+e$, then there exist such $m > 0$ and $n > 0$, that $(e+e)^m = (e+e)^{m+n}$. Thus $(e+e)^{m+n} - (e+e)^n = 0$, i.e.,

$$\begin{aligned} 0 &= (e+e)^{m+n} - (e+e)^n \\ &= \sum_{s=0}^{m+n} \binom{m+n}{s} e - \sum_{\sigma=0}^{n} \binom{n}{\sigma} e \\ &= \left(\sum_{s=0}^{m+n} \binom{m+n}{s} - \sum_{\sigma=0}^{n} \binom{n}{\sigma} \right) e. \end{aligned}$$

Here $ke = \underbrace{e + e + \cdots + e}_{k}$. Note that $2e$ is not idempotent. If the contrary is true, then $e + e = (e+e)^2 = e^2 + 2e + e^2 = e + 2e + e$. Hence $e + e = 0$. $\blacksquare$

2.9. Proposition. *If* $\mathrm{char}(R) = m \neq 0$*, then there exist such subring G of ring R, that G is isomorph to ring $\mathbb{Z}_m$.*

□ Let's define set $G \leftharpoondown \{ke \,|\, k \in \mathbb{N}\}$, here e is the unit element of ring R. If

$$\begin{aligned} k+n &= mq_1 + r_1, \quad 0 \le r_1 < m; \\ kn &= mq_2 + r_2, \quad 0 \le r_2 < m, \end{aligned}$$

then

$$\begin{aligned} (k+n)e &= (mq_1 + r_1)e = q_1(me) + r_1 e = r_1 e, \\ kne &= (mq_2 + r_2)e = q_2(me) + r_2 e = r_2 e. \end{aligned}$$

In $\mathbb{Z}_m$ we have

$$\begin{aligned} k+n &\equiv r_1 \mod m, \\ kn &\equiv r_2 \mod m. \end{aligned}$$

Hence mapping $f : G \to \mathbb{Z}_m : ke \mapsto k$ is an isomorphism of rings. ■

We will use 1 instead of e, unless it may cause misunderstandings.

2.10. Definition. *Consider a commutative ring with unity R. Extension G of R is called an integral extension, if for each $c \in G$, there exists such monic polynomial $p(X) \in R[X]$, that $p(c) = 0$.*

2.11. Proposition. *A periodic ring is an integral extension of $\mathbb{Z}_m$ (up to isomorphism).*

□ Assume that R is periodical and $a \in R$. From (2.8. corollary) and (2.9. Proposition) there exist such m, that R contains a subring isomorph to ring $\mathbb{Z}_m$. As R is periodic, then there exists such $0 < k < n$, that $a^k = a^n$. Thus a is the root of the monic polynomial $X^n - X^{n-k}$. ■

2.12. Lemma. *If $\mathcal{I} \subseteq \mathcal{J}$ are ideal of ring R, then mapping*

$$f : R/\mathcal{I} \to R/\mathcal{J} : x + \mathcal{I} \mapsto x + \mathcal{J}$$

is an epimorphism of rings.

□ (i) Let's show that mapping f is defined correctly. Assume that $x+\mathcal{I} = y+\mathcal{I}$, then $x-y \in \mathcal{I}$ and therefore $x-y \in \mathcal{J}$. Hence $x+\mathcal{J} = y+\mathcal{J}$.

(ii) Let's introduce notation:

$$\begin{aligned} [x]_{\mathcal{I}} &\leftharpoondown x + \mathcal{I}, \\ [x]_{\mathcal{J}} &\leftharpoondown x + \mathcal{J}, \end{aligned}$$

then

$$\begin{aligned} f[x+y]_{\mathcal{I}} &= [x+y]_{\mathcal{J}} = [x]_{\mathcal{J}} + [y]_{\mathcal{J}} = f[x]_{\mathcal{I}} + f[y]_{\mathcal{I}}, \\ f[xy]_{\mathcal{I}} &= [xy]_{\mathcal{J}} = [x]_{\mathcal{J}}[y]_{\mathcal{J}} = f[x]_{\mathcal{I}} f[y]_{\mathcal{I}}, \\ f[1]_{\mathcal{I}} &= [1]_{\mathcal{J}}. \end{aligned}$$

Thus f is a homomorphism of rings.

(iii) Assume that $[x]_{\mathcal{J}} \in R/\mathcal{J}$, then

$$[x]_{\mathcal{J}} = x + \mathcal{J} \supseteq x + \mathcal{I} = [x]_{\mathcal{I}}.$$

Thus $f[x]_{\mathcal{I}} = [x]_{\mathcal{J}}$, e.i, f is surjective. ■

Let's denote principal ideal $g(X)R[X]$ as $\langle g(X) \rangle$.

2.13. Lemma. *If R is a finite commutative local ring and*

$$g(X) = 1 + a_1X + a_2X^2 + \cdots + a_kX^k \in R[X],$$

then $|R[X]/\langle g(X)\rangle| < \infty$.

$\square$ (i) Assume that $\mathfrak{M}$ is maximal ideal of ring R, $a_t \in R^\times$, but

$$a_{t+1}, a_{t+2}, \ldots, a_k \notin R^\times,$$

thus (1.42. Proposition) $a_{t+1}, a_{t+2}, \ldots, a_k \in \mathfrak{M}$.

(ii) Maximal ideal $\mathfrak{M}$ of ring R is prime (1.20. Corollary). If $\mathcal{I}$ is a prime ideal of finite ring R, then it is maximal (1.27. Corollary). In the given case, this means we have only one prime ideal, e.i., $\mathfrak{M}$. As R is commutative ring, then (1.32. Proposition)

$$Nil(R) = \bigcap_{\mathcal{I}\in \mathrm{Spec}(R)} \mathcal{I}.$$

Here

- $Nil(R)$ is a nilradical, e.i., a set consisting of all nilpotent elements of R;
- $Spec(R)$ is a spectrum of ring R spektrs, e.i., set of all prime ideals.

In this case $Nil(R) = \mathfrak{M}$. Thus (1.33. Lemma) there exist such l, that $(Nil(R))^l = \mathfrak{M}^l = 0$. Note that R here is a finite ring.

(iii) Let $g_1(X) \Leftarrow (1+a_1X+a_2X^2+\cdots+a_tX^t)^l$. For any commutative ring holds

$$\alpha^l - \beta^l = (\alpha - \beta)\sum_{i=1}^{l} \alpha^{l-i}\beta^{i-1}.$$

If

- α is given as $1 + a_1X + a_2X^2 + \cdots + a_tX^t$,
- β is given as $-\sum_{i=t+1}^{k} a_iX^i$,

then $\alpha - \beta = g(X)$ and thus $g(X)$ divides polynomial

$$(1 + a_1X + a_2X^2 + \cdots + a_tX^t)^l - (-\sum_{i=t+1}^{k} a_iX^i)^l.$$

As $\mathfrak{M}^l = 0$, then all coeficient of polynomial $(-\sum_{i=t+1}^{k} a_iX^i)^l$ are equal to 0, because $a_{t+1}, a_{t+2}, \ldots, a_k \in \mathfrak{M}$. Hence

$$g_1(X) = (1 + a_1X + a_2X^2 + \cdots + a_tX^t)^l - (-\sum_{i=t+1}^{k} a_iX^i)^l.$$

(iv) Lets rewrite $g_1(X)$ as $1 + b_1X + \cdots + b_uX^u$. Here $u = tl$ and $b_u = a_t^u \in R^\times$. Hence $|R[X]/\langle g_1(X)\rangle| = |R|^u < \infty$. Note that

$$\begin{array}{rcl} R[X]/g_1(X) & = & \{[r(X)] \mid h(X) \in R[X] \\ & \wedge & h(X) = f(X)g_1(X) + r(X) \\ & \wedge & \deg(r(X)) < \deg(g_1(X)) = u\} \end{array}$$

(v) If $a = bc$, then $aR \subseteq bR$. Thus if $x \in aR$, then $x = ar$, where $r \in R$ and $x = ar = bcr \in bR$.

As $g(X)$ divides $g_1(X)$, then $\langle g_1(X) \rangle = g_1(X)R[X] \subseteq g(X)R[X] = \langle g(X) \rangle$. From (2.12. Lemma) mapping

$$f : R[X]/\langle g_1(X) \rangle \to R[X]/\langle g(X) \rangle : p(X) + \langle g_1(X) \rangle \mapsto p(X) + \langle g(X) \rangle$$

is surjective. Thus $|R[X]/\langle g_1(X) \rangle| \geq |R[X]/\langle g(X) \rangle|$, i.e., $|R|^u \geq |R[X]/\langle g(X) \rangle|$. ■

Let R and G be rings and $\varphi : R \to G^n$ be a ring isomorphism. Let $\bar{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$, where

$$a_{ij} = \begin{cases} a_i, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases}$$

Thus $(a_1, a_2, \ldots, a_n) = \bar{a}_1 + \bar{a}_2 + \cdots + \bar{a}_n$. As φ is an isomorphism, then $\varphi^{-1} : G^n \to R$ also is an isomorphism. Hence

$$\begin{aligned} \varphi^{-1}(a_1, a_2, \ldots, a_n) &= \varphi^{-1}(\bar{a}_1 + \bar{a}_2 + \cdots + \bar{a}_n) \\ &= \varphi^{-1}(\bar{a}_1) + \varphi^{-1}(\bar{a}_2) + \cdots + \varphi^{-1}(\bar{a}_n). \end{aligned}$$

Let $\bar{e}_i = (e_{i1}, e_{i2}, \ldots, e_{in})$, where

$$e_{ij} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases}$$

Thus $(1, 1, \ldots, 1) = \bar{e}_1 + \bar{e}_2 + \cdots + \bar{e}_n$. Hence

$$\begin{aligned} 1 &= \varphi^{-1}(1, 1, \ldots, 1) = \varphi^{-1}(\bar{e}_1 + \bar{e}_2 + \cdots + \bar{e}_n) \\ &= \varphi^{-1}(\bar{e}_1) + \varphi^{-1}(\bar{e}_2) + \cdots + \varphi^{-1}(\bar{e}_n). \end{aligned}$$

2.14. Lemma. *If $\phi : R \to S$ is a homomorphism of rings, then*

$$\phi : R[X] \to S[X] : \sum_{i=0}^{m} a_i X^i \mapsto \sum_{i=0}^{m} \phi(a_i) X^i$$

is a homomorphism of rings.

$$\begin{aligned} \square \quad \phi(\sum_{i=0}^{m}(a_i + b_i)X^i) &= \sum_{i=0}^{m} \phi(a_i + b_i)X^i = \sum_{i=0}^{m}(\phi(a_i) + \phi(b_i))X^i \\ &= \sum_{i=0}^{m} \phi(a_i)X^i + \sum_{i=0}^{m} \phi(b_i)X^i \\ &= \phi(\sum_{i=0}^{m} a_i X^i) + \phi(\sum_{i=0}^{m} b_i X^i). \end{aligned}$$

$$
\begin{aligned}
\phi((\sum_{i=0}^{m} a_i X^i)(\sum_{j=0}^{n} b_j X^j)) &= \phi(\sum_{k=0}^{m+n}(\sum_{s=0}^{k} a_s b_{k-s})X^k) \\
&= \sum_{k=0}^{m+n} \phi(\sum_{s=0}^{k} a_s b_{k-s})X^k \\
&= \sum_{k=0}^{m+n} \sum_{s=0}^{k} \phi(a_s)\phi(b_{k-s})X^k \\
&= (\sum_{i=0}^{m} \phi(a_i)X^i)(\sum_{j=0}^{n} \phi(b_j)X^j) \\
&= \phi(\sum_{i=0}^{m} a_i X^i)\phi(\sum_{j=0}^{n} b_j X^j). \quad \blacksquare
\end{aligned}
$$

Thus we have proven:

- $\phi(p+q) = \phi(p) + \phi(q)$,
- $\phi(pq) = \phi(p)\phi(q)$

for all $p, q \in R[X]$.

2.15. Corollary. (i) *If $\phi : R \to S$ is a ring epimorphism, then $\phi : R[X] \to S[X] : \sum_{i=0}^{m} a_i X^i \mapsto \sum_{i=0}^{m} \phi(a_i) X^i$ is a ring epimorphism.*
(ii) *If $\phi : R \to S$ is a ring monomorphism, then $\phi : R[X] \to S[X] : \sum_{i=0}^{m} a_i X^i \mapsto \sum_{i=0}^{m} \phi(a_i) X^i$ is a ring monomorphism.*
(iii) *If $\phi : R \to S$ is a ring isomorphism, then $\phi : R[X] \to S[X] : \sum_{i=0}^{m} a_i X^i \mapsto \sum_{i=0}^{m} \phi(a_i) X^i$ is a ring isomorphism.*

□ (i) Let $\sum_{i=0}^{m} \alpha_i X^i \in S[X]$. As $\phi : R \to S$ is an epimorphism, then exist such $a_1, a_2, \ldots, a_m \in R$, that $\forall i \; \phi(a_i) = \alpha_i$. Hence $\phi(\sum_{i=0}^{m} a_i X^i) = \sum_{i=0}^{m} \alpha_i X^i$.
(ii) Let $\sum_{i=0}^{m} a_i X^i \neq \sum_{i=0}^{m} b_i X^i$. Thus there exists such k, that $a_k \neq b_k$. Hence $\sum_{i=0}^{m} \phi(a_i) X^i \neq \sum_{i=0}^{m} \phi(b_i) X^i$.
(iii) Follows as a consequence of (i) and (ii). ■

2.16. Lemma. *If $\phi : R \to S$ is a ring isomorphism, then*

$$R[X]/\langle \sum_{i=0}^{m} a_i X^i \rangle \cong S[X]/\langle \sum_{i=0}^{m} \phi(a_i) X^i \rangle.$$

□ Let $\sum_{i=0}^{n} b_i X^i \equiv_R \sum_{i=0}^{n} c_i X^i$, i.e.., they represent the same element of set $R[X]/\langle \sum_{i=0}^{m} a_i X^i \rangle$. There is a possibility of polynomials $\sum_{i=0}^{n} b_i X^i$ and $\sum_{i=0}^{n} c_i X^i$ to have different orders, then some of the coefficients are equal to 0.

Let's denote polynomials in consideration as: $f \leftharpoondown \sum_{i=0}^{m} a_i X^i$, $\phi(f) \leftharpoondown \sum_{i=0}^{m} \phi(a_i) X^i$, $p \leftharpoondown \sum_{i=0}^{n} b_i X^i$, $q \leftharpoondown \sum_{i=0}^{n} c_i X^i$.

Then

$$
\begin{array}{rcl}
p & \equiv_R & q, \\
p - q & \equiv_R & 0, \\
\exists r \in R[X]\ fr & = & p - q, \\
\phi(r)\phi(f) = \phi(rf) & = & \phi(p - q) = \phi(p) - \phi(q), \\
\phi(p) - \phi(q) & \equiv_S & 0, \\
\phi(p) & \equiv_S & \phi(q).
\end{array}
$$

As mapping $\phi : R \to S$ is an isomorpism, then $p \equiv_R q \Leftrightarrow \phi(p) \equiv_S \phi(q)$. Hence mapping $\bar{\phi} : R[X]/f \to S[X]/\phi(f) : [p]_R \to [\phi(p)]_S$ is bijectivre. Here

$$[p]_R \leftleftharpoons \{g \mid g \equiv_R p\}, \qquad [\phi(p)]_S \leftleftharpoons \{h \mid h \equiv_S \phi(p)\}.$$

$$
\begin{array}{rcl}
\bar{\phi}([p]_R[q]_R) & = & \bar{\phi}([pq]_R) = [\phi(pq)]_S = [\phi(p)\phi(q)]_S \\
& = & [\phi(p)]_S[\phi(q)]_S = \bar{\phi}([p]_R)\bar{\phi}([q]_R), \\
\bar{\phi}([p]_R + [q]_R) & = & \bar{\phi}([p+q]_R) = [\phi(p+q)]_S = [\phi(p) + \phi(q)]_S \\
& = & [\phi(p)]_S + [\phi(q)]_S = \bar{\phi}([p]_R) + \bar{\phi}([q]_R).
\end{array}
$$

Thus $\bar{\phi}$ is an isomorphism. ■

2.17. Lemma. *If $\phi : R \mapsto G_1 \times G_2 \times \cdots \times G_n$ is a ring homomorphism, then for all i*

$$\phi_i : R \to G_i : r \mapsto \mathrm{pr}_i(\phi(r))$$

is a ring homomorphism. Here $\mathrm{pr}_i(r_1, r_2, \ldots, r_n) \leftleftharpoons r_i$.

□ Let $\phi(x) = (x_1, x_2, \ldots, x_n)$ and $\phi(y) = (y_1, y_2, \ldots, y_n)$, then

$$
\begin{array}{rcl}
\phi_i(x+y) & = & \mathrm{pr}_i(\phi(x+y)) = \mathrm{pr}_i(\phi(x) + \phi(y)) = x_i + y_i \\
& = & \phi_i(x) + \phi_i(y); \\
\phi_i(xy) & = & \mathrm{pr}_i(\phi(xy)) = \mathrm{pr}_i(\phi(x)\phi(y)) = x_i y_i \\
& = & \phi_i(x)\phi_i(y). \quad ■
\end{array}
$$

2.18. Proposition. *If $\phi : R \to G_1 \times G_2 \times \cdots \times G_n$ is a ring isomorphism and $f = \sum_{j=0}^{m} a_j X^j \in R[X]$, then*

$$R[X]/\langle f \rangle \cong G_1[X]/\langle \phi_1(f) \rangle \times G_2[X]/\langle \phi_2(f) \rangle \times \cdots \times G_n[X]/\langle \phi_n(f) \rangle.$$

Here $\quad \phi_i(f) \leftleftharpoons \sum_{j=0}^{m} \mathrm{pr}_i(\phi(a_j))X^j$.

□ (i) Mapping $\phi_i : R \to G_i : r \mapsto \mathrm{pr}_i(\phi(r))$ is ring homomorphism (2.17. Lemma). As ϕ is an isomorphism, then ϕ_i is an epimorphism. Thus (2.15. Corollary)

$$\phi_i : R[X] \to G_i[X] : p \mapsto \phi_i(p)$$

is an epimorphism.

Assume that $\sum_{j=0}^{\nu} b_j X^j \equiv_R \sum_{j=0}^{\nu} c_j X^j$, i.e,, they represent the same element from set $R[X]/\langle\sum_{j=0}^{m} a_j X^j\rangle$. Let's denote polynomials in consideration as: $p \leftharpoondown\!\!\!= \sum_{j=0}^{\nu} b_j X^j$, $q \leftharpoondown\!\!\!= \sum_{j=0}^{\nu} c_j X^j$. Then

$$\begin{array}{rcl} p & \equiv_R & q, \\ p - q & \equiv_R & 0, \\ \exists r \in R[X]\ fr & = & p - q, \\ \phi_i(r)\phi_i(f) = \phi_i(rf) & = & \phi_i(p-q) = \phi_i(p) - \phi_i(q), \\ \phi_i(p) - \phi_i(q) & \equiv_{G_i} & 0, \\ \phi_i(p) & \equiv_{G_i} & \phi_i(q). \end{array}$$

This shows that mappings

$$\bar{\phi}_i : R[X]/\langle f\rangle \to G_i[X]/\langle \phi_i(f)\rangle : [p]_R \mapsto [\phi_i(p)]_{G_i}$$

are defined correctly. Here

$$[p]_R \leftharpoondown\!\!\!= \{g \mid g \equiv_R p\}, \qquad [\phi_i(p)]_{G_i} \leftharpoondown\!\!\!= \{h \mid h \equiv_{G_i} \phi_i(p)\}.$$

$$\begin{array}{rcl} \bar{\phi}_i([p]_R[q]_R) & = & \bar{\phi}_i([pq]_R) = [\phi_i(pq)]_{G_i} = [\phi_i(p)\phi_i(q)]_{G_i} \\ & = & [\phi_i(p)]_{G_i}[\phi_i(q)]_{G_i} = \bar{\phi}_i([p]_R)\bar{\phi}_i([q]_R), \\ \bar{\phi}_i([p]_R + [q]_R) & = & \bar{\phi}_i([p+q]_R) = [\phi_i(p+q)]_{G_i} = [\phi_i(p) + \phi_i(q)]_{G_i} \\ & = & [\phi_i(p)]_{G_i} + [\phi_i(q)]_{G_i} = \bar{\phi}_i([p]_R) + \bar{\phi}_i([q]_R). \end{array}$$

Hence $\bar{\phi}_i$ is a homomorphism. Thus

$$\bar{\phi} : [p]_R \mapsto (\bar{\phi}_1([p]_R), \bar{\phi}_2([p]_R), \ldots, \bar{\phi}_n([p]_R))$$

is a homomorphism.

(ii) Let $p_i \in G_i[X]$ and $k = \max_i \deg(p_i)$. Thus

$$p_i(X) = \sum_{j=0}^{k} a_{ij} X^j \in G_i[X].$$

As ϕ is bijective, then there exist such r_s, $s \in \overline{1,k}$, that

$$\phi(r_s) = (a_{1s}, a_{2s}, \ldots, a_{ns}).$$

Lets choose $p(X) \leftharpoondown\!\!\!= \sum_{j=0}^{k} r_j X^j$. Thus mapping

$$\Phi : R[X] \to G_1[X] \times G_2[X] \times \cdots \times G_n[X] : p \mapsto (\phi_1(p), \phi_2(p), \ldots, \phi_n(p))$$

is surjective. As $\deg(\phi_i(p)) = \deg(p)$, then only case, when Φ is not injective, might arise when $p \neq q$, but $\deg(p) = \deg(q)$. Let $q(X) = \sum_{j=0}^{k} \rho_j X^j$, $r_\varkappa \neq \rho_\varkappa$ and $\phi(\rho_\varkappa) = (b_1, b_2, \ldots, b_n)$. In expanded expression:

$$(a_{1\varkappa}, a_{2\varkappa}, \ldots, a_{n\varkappa}) = \phi(r_\varkappa) \neq \phi(\rho_\varkappa) = (b_1, b_2, \ldots, b_n).$$

Thus there exist such ν, that $a_{\nu\varkappa} \neq b_\nu$.

$$\begin{aligned}
\phi_\nu(p) &= \sum_{j=0}^{k} \phi_\nu(r_j) X^j = \sum_{j=0}^{k} a_{\nu j} X^j = \sum_{j\neq\varkappa} a_{\nu j} X^j + a_{\nu\varkappa} X^\varkappa. \\
\phi_\nu(q) &= \sum_{j=0}^{k} \phi_\nu(\rho_j) X^j = \sum_{j\neq\varkappa} \phi_\nu(\rho_j) X^j + \phi_\nu(\rho_\varkappa) X^\varkappa \\
&= \sum_{j\neq\varkappa} \phi_\nu(\rho_j) X^j + b_\nu X^\varkappa.
\end{aligned}$$

Thus $\phi_\nu(p) \neq \phi_\nu(q)$, i.e., Φ is injective. From all the above, we conclude that Φ is bijective.

(iii) Let

$$\begin{aligned}
&([p_1]_{G_1}, [p_2]_{G_2}, \ldots, [p_n]_{G_n}) \in \\
&G_1[X]/\langle\phi_1(f)\rangle \times G_2[X]/\langle\phi_2(f)\rangle \times \cdots \times G_n[X]/\langle\phi_n(f).
\end{aligned}$$

Thus $[p_i] \subseteq G_i[X]$ and $p_i \in G_i[X]$. As Φ is bijective, then exist such $p \in R[X]$, that $\Phi(p) = (p_1, p_2, \ldots, p_n)$, e.i.,

$$p_1 = \phi_1(p), p_2 = \phi_2(p), \ldots, p_n = \phi_n(p).$$

Hence $[p_i]_{G_i} = [\phi_i(p)]_{G_i}$. From the definition of $\bar{\phi}_i$, we have $\bar{\phi}_i : [p]_R \mapsto [\phi_i(p)]_{G_i}$ and

$$\begin{aligned}
\bar{\phi} : [p]_R &\mapsto (\bar{\phi}_1([p]_R), \bar{\phi}_2([p]_R), \ldots, \bar{\phi}_n([p]_R)) \\
&= ([p_1]_{G_1}, [p_2]_{G_2}, \ldots, [p_n]_{G_n}).
\end{aligned}$$

Hence $\bar{\phi}$ is surjective.

Let $\bar{\phi}([p]_R) = \bar{\phi}([0]_R)$, then $\forall i$ $\bar{\phi}_i([p]_R) = \bar{\phi}_i([0]_R)$, t.i., $[\phi_i(p)]_{G_i} = [\phi_i(0)]_{G_i} = [0]_{G_i}$. Thus there exist such $r_i \in G_i[X]$, that $\phi_i(p) = r_i\phi_i(f)$. As

$$\Phi : R[X] \to G_1[X] \times G_2[X] \times \cdots \times G_n[X]$$

is bijective, then exists $\rho \in R[X]$, that $\Phi(\rho) = (r_1, r_2, \ldots, r_n)$. On the other hand $\Phi(\rho) = (\phi_1(\rho), \phi_2(\rho), \ldots, \phi_n(\rho))$. Thus $r_i = \phi_i(\rho)$, therefore $\phi_i(p) = r_i\phi_i(f) = \phi_i(\rho)\phi_i(f) = \phi_i(\rho f)$. Hence

$$\Phi(p) = (\phi_1(p), \phi_2(p), \ldots, \phi_n(p)) = (\phi_1(\rho f), \phi_2(\rho f), \ldots, \phi_n(\rho f)) = \Phi(\rho f).$$

Mapping Φ is bijective, therefore $p = \rho f$, t.i., $[p]_R = [0]_R$. Thus the kernel of homomorphism $\bar{\phi}$ is trivial, hence $\bar{\phi}$ is a monomorphism.

From all the above we conclude:

$$\bar{\phi} : R[X]/\langle f\rangle \to G_1[X]/\langle\phi_1(f)\rangle \times G_2[X]/\langle\phi_2(f)\rangle \times \cdots \times G_n[X]/\langle\phi_n(f)\rangle$$

is an isomorphism. ■

2.19. Lemma. *Let $g(X) = 1 + a_1X + a_2X^2 + \cdots + a_kX^k \in R[X]$. If R is integral extension of ring $\mathcal{Z}_m \cong \mathbb{Z}_m$, then there exist such n, that $g(X)$ divides $X^n - 1$.*

□ (i) Let $\alpha = aa_1^{s_1}a_2^{s_2}\dots a_k^{s_k}, \beta = ba_1^{s_1}a_2^{s_2}\dots a_k^{s_k}$, where $a, b \in \mathcal{Z}_m$, then $\alpha + \beta = (a+b)a_1^{s_1}a_2^{s_2}\dots a_k^{s_k}$ and $a + b \in \mathcal{Z}_m$. Let denote by $\mathcal{Z}_m(a_1, a_2, \dots, a_k)$ the smallest extension of ring $\mathcal{Z}_m$, containing all elements $a_1, a_2, \dots, a_k$. Thus $\mathcal{Z}_m(a_1, a_2, \dots, a_k)$ consists of sums:

$$\sum_{\bar{\varkappa}\in\mathcal{Z}_m} a_{\bar{\varkappa}} a_1^{\varkappa_1} a_2^{\varkappa_2}\dots a_k^{\varkappa_k},$$

where $a_{\bar{\varkappa}} \in \mathcal{Z}_m$ and $\bar{\varkappa} = (\varkappa_1, \varkappa_2, \dots, \varkappa_k)$. There all $\bar{\varkappa}$ are distinct.

(ii) As $\mathcal{Z}_m(a_1, a_2, \dots, a_k)$ is an integral extension, then for each a_i there exists such monic polinomial

$$p_i(X) = X^{m_i} + b_{im_i-1}X^{m_i-1} + \dots + b_{i2}X^2 + b_{i1}X + b_{i0},$$

that $p_i(a_i) = 0$. Hence

$$a_i^{m_i} = -b_{im_i-1}a_i^{m_i-1} - \dots - b_{i2}a_i^2 - b_{i1}a_i - b_{i0}.$$

Thus each element of ring $\mathcal{Z}_m(a_1, a_2, \dots, a_k)$ is representable as a sum

$$\sum_{\bar{\varkappa}\in\mathcal{Z}_m} a_{\bar{\varkappa}} a_1^{\varkappa_1} a_2^{\varkappa_2}\dots a_k^{\varkappa_k},$$

where all $\bar{\varkappa} = (\varkappa_1, \varkappa_2, \dots, \varkappa_k)$ are distinct and all $\varkappa_i < m_i$. Then count of such sums is finite, because ring $\mathcal{Z}_m$ is finite. Thus ring $\mathcal{Z}_m(a_1, a_2, \dots, a_k)$ is finite.

(iii) As $S \leftrightharpoons \mathcal{Z}_m(a_1, a_2, \dots, a_k)$ is a finite ring, then (1.45. Theorem)

$$S \cong S_1 \times S_2 \times \dots \times S_t,$$

where all S_i are finite commutative rings. Thus (2.18. Proposition)

$$S[X]/\langle g\rangle \cong S_1[X]/\langle\phi_1(g)\rangle \times S_2[X]/\langle\phi_2(g)\rangle \times \dots \times S_t[X]/\langle\phi_t(g)\rangle.$$

Here

$$\bar{\phi} : S[X]/\langle g\rangle \to S_1[X]/\langle\phi_1(g)\rangle \times S_2[X]/\langle\phi_2(g)\rangle \times \dots \times S_t[X]/\langle\phi_t(g)\rangle$$

is an isomorphism, where

$$\phi : S \to S_1 \times S_2 \times \dots \times S_t$$

is an isomorphism, $\phi_i(g) = \sum_{j=0}^{k} \mathrm{pr}_i(\phi(a_j))X^j$ and $a_0 = 1$. Thus

$$\phi_i(g) = 1_{S_i} + \sum_{j=1}^{k} \mathrm{pr}_i(\phi(a_j))X^j.$$

(2.13. Lemma) $S_i[X]/\langle\phi_i(g)\rangle$ is a finite set, thus $S[X]/\langle g\rangle$ is a finite ring. Therefore all classes $[1], [X], [X^2], [X^3], \dots, [X^s], \dots$ can't be distinct. Thus there exist such $\nu \geq 0$ and $n > 0$, that $[X^\nu] = [X^{\nu+n}]$ or $[X^\nu(X^n - 1)] = [0]$. Thus thre exist such $q(X) \in S[X]$, that $g(X)q(X) = X^\nu(X^n - 1)$. As $g(0) = 1$, then $q(X) = X^\nu r(X)$. Hence $X^\nu g(X)r(X) = X^\nu(X^n - 1)$. It is possible only if $g(X)r(X) = X^n - 1$. ■

2.20. Proposition. *If integral extension f of $\mathcal{Z}_m \cong \mathbb{Z}_m$ is a rational series, then f is semiperiodic.*

$\square$ Let R be extension of ring $\mathcal{Z}_m$, $f(X) = \frac{h(X)}{g(X)}$ and $g(X) = \sum_{k=0}^{\nu} a_k X^k$, then $g(X) = a_0(1 + \sum_{k=1}^{\nu} a_0^{-1} a_k X^k)$. Thus (2.19. Lemma) exists such n, that $X^n - 1 = a_0^{-1} g r$, where $r \in R[X]$. Hence

$$\begin{aligned} f &= \frac{h}{g} = \frac{h(X^n-1)}{g(X^n-1)} = \frac{a_0^{-1}h}{X^n-1} \cdot \frac{X^n-1}{a_0^{-1}g} = \frac{a_0^{-1}h}{X^n-1} \cdot \frac{a_0^{-1}gr}{a_0^{-1}g} \\ &= \frac{a_0^{-1}hr}{X^n-1} = -a_0^{-1}hr \sum_{k=0}^{\infty} X^{kn} \end{aligned}$$

Assume that $-a_0^{-1}hr = \sum_{\varkappa=0}^{\sigma} b_\varkappa X^\varkappa$, then $f = \sum_{\varkappa=0}^{\sigma} b_\varkappa X^\varkappa \sum_{k=0}^{\infty} X^{kn}$. If $n = 1$, then

$$\begin{aligned} f &= \sum_{\varkappa=0}^{\sigma} b_\varkappa X^\varkappa \sum_{k=0}^{\infty} X^k \\ &= (b_0 + b_1 X + b_2 X^2 \ldots + b_\sigma X^\sigma)(1 + X + X^2 + \ldots + X^\sigma + \ldots) \\ &= b_0 + (b_0 + b_1)X + (b_0 + b_1 + b_2)X^2 + \ldots + (b_0 + b_1 + \ldots + b_\sigma)X^\sigma \\ &+ (b_0 + b_1 + \ldots + b_\sigma)X^{\sigma+1} + \ldots + (b_0 + b_1 + \ldots + b_\sigma)X^{\sigma+n} + \ldots \\ &= \sum_{k=0}^{\sigma-1}\Big(\sum_{i=0}^{k} b_i\Big)X^k + \sum_{n=0}^{\infty}\Big(\sum_{i=0}^{\sigma} b_i\Big)X^{\sigma+n} \end{aligned}$$

If $\sigma < n$, then

$$\begin{aligned} f &= \sum_{\varkappa=0}^{\sigma} b_\varkappa X^\varkappa \sum_{k=0}^{\infty} X^{kn} \\ &= (b_0 + b_1 X + b_2 X^2 \ldots + b_\sigma X^\sigma)(1 + X^n + X^{2n} + \ldots + X^{kn} + \ldots) \\ &= b_0 + b_1 X + b_2 X^2 + \ldots + b_\sigma X^\sigma \\ &+ b_0 X^n + b_1 X^{n+1} + b_2 X^{n+2} + \ldots + b_\sigma X^{n+\sigma} \\ &+ b_0 X^{2n} + b_1 X^{2n+1} + b_2 X^{2n+2} + \ldots + b_\sigma X^{2n+\sigma} + \ldots \\ &= \sum_{k=0}^{\infty}\sum_{i=0}^{\sigma} b_i X^{kn+i} \end{aligned}$$

If $\sigma = n + \tau$ un $0 \le \tau < n$, then

$$\begin{aligned} f &= \sum_{\varkappa=0}^{\sigma} b_\varkappa X^\varkappa \sum_{k=0}^{\infty} X^{kn} \\ &= (b_0 + b_1 X + b_2 X^2 \ldots + b_{n-1}X^{n-1} + b_n X^n + \ldots + b_{n+\tau}X^{n+\tau}) \\ &\times (1 + X^n + X^{2n} + \ldots + X^{kn} + \ldots) \\ &= b_0 + b_1 X + b_2 X^2 + \ldots + b_{n-1}X^{n-1} \\ &+ (b_0 + b_n)X^n + (b_1 + b_{n+1})X^{n+1} + \ldots + (b_\tau + b_{n+\tau})X^{n+\tau} \\ &+ b_{\tau+1}X^{n+\tau+1} + b_{\tau+2}X^{n+\tau+2} + \ldots + b_{n-1}X^{2n-1} \\ &+ (b_0 + b_n)X^{2n} + (b_1 + b_{n+1})X^{2n+1} + \ldots + (b_\tau + b_{n+\tau})X^{2n+\tau} \end{aligned}$$

$$
\begin{aligned}
+ \quad & b_{\tau+1}X^{2n+\tau+1} + b_{\tau+2}X^{2n+\tau+2} + \ldots + b_{n-1}X^{3n-1} + \ldots \\
= \quad & \sum_{k=0}^{n-1} b_k X^k + \sum_{k=1}^{\infty}\Big(\sum_{i=0}^{\tau}(b_i + b_{n+i})X^{kn+i} + \sum_{i=\tau+1}^{n-1} b_i X^{kn+i}\Big)
\end{aligned}
$$

If $\sigma = mn + \tau$ un $0 \le \tau < n$, then

$$
\begin{aligned}
f \quad = \quad & \sum_{\varkappa=0}^{\sigma} b_\varkappa X^\varkappa \sum_{k=0}^{\infty} X^{kn} \\
= \quad & (b_0 + b_1 X + b_2 X^2 \ldots + b_{n-1}X^{n-1} + b_n X^n + \ldots + b_{mn+\tau}X^{mn+\tau}) \\
\times \quad & (1 + X^n + X^{2n} + \ldots + X^{kn} + \ldots) \\
= \quad & b_0 + b_1 X + b_2 X^2 + \ldots + b_{n-1}X^{n-1} \\
+ \quad & (b_0 + b_n)X^n + (b_1 + b_{n+1})X^{n+1} + \ldots + (b_{n-1} + b_{2n-1})X^{2n-1} + \\
\ldots \quad & +(b_0 + b_n + b_{2n} \ldots + b_{(m-1)n})X^{(m-1)n} \\
+ \quad & (b_1 + b_{n+1} + b_{2n+1} + \ldots + b_{(m-1)n+1})X^{(m-1)n+1} + \ldots \\
+ \quad & (b_{n-1} + b_{2n-1} + b_{3n-1} + \ldots + b_{mn-1})X^{mn-1} \\
+ \quad & (b_0 + b_n + \ldots + b_{mn})X^{mn} + (b_1 + b_{n+1} + \ldots + b_{mn+1})X^{mn+1} + \\
\ldots \quad & +(b_\tau + b_{n+\tau} + \ldots + b_{mn+\tau})X^{mn+\tau} \\
+ \quad & (b_{\tau+1} + b_{n+\tau+1} + \ldots + b_{(m-1)n+\tau+1})X^{mn+\tau+1} + \ldots \\
= \quad & \sum_{k=0}^{m-1}\sum_{i=0}^{n-1}\Big(\sum_{j=0}^{k} b_{i+jn}\Big)X^{nk+i} \\
+ \quad & \sum_{k=m}^{\infty}\Big(\sum_{i=0}^{\tau}\Big(\sum_{j=0}^{m} b_{i+jn}\Big)X^{kn+i} + \sum_{i=\tau+1}^{n-1}\Big(\sum_{j=0}^{m-1} b_{i+jn}\Big)X^{kn+i}\Big) \quad \blacksquare
\end{aligned}
$$

2.21. Corollary. *Each formal power series of a periodic ring is semiperiodic.*

□ Periodic ring is integral extension of ring $\mathbb{Z}_m$ (2.11. Proposition), up to isomorphism. The result follows from (2.20. Proposition). ■

2.22. Example. $f(X) = \frac{X^2+2X-1}{X^2+X+1}$, *where polinomials are elements of ring* $\mathbb{Z}_6[X]$.

$$
\begin{aligned}
f(X) \quad = \quad & \frac{X^2 + 2X - 1}{X^2 + X + 1} = \frac{(X^2 + 2X - 1)(X^3 - 1)}{(X^2 + X + 1)(X^3 - 1)} \\
= \quad & \frac{(X^2 + 2X - 1)(X - 1)}{X^3 - 1} \\
= \quad & -(1 - 3X + X^2 + X^3)(1 + X^3 + X^6 + X^9 + \ldots)
\end{aligned}
$$

Let's consider the general expression: $\sigma = n = 3$ and $\tau = 0$.

$$
\begin{aligned}
f(X) \quad = \quad & (b_0 + b_1 X + b_2 X^2 + b_3 X^3)(1 + X^3 + X^6 + X^9 + \ldots) \\
= \quad & b_0 + b_1 X + b_2 X^2 + \sum_{k=1}^{\infty}\big((b_0 + b_3)X^{3k} + b_1 X^{3k+1} + b_2 X^{3k+2}\big)
\end{aligned}
$$

In our case:

$$\begin{aligned} f(X) &= -1+3X-X^2+\sum_{k=1}^{\infty}\big((-1-1)X^{3k}+3X^{3k+1}-X^{3k+2}\big) \\ &= -1+3X-X^2+\sum_{k=1}^{\infty}\big(-2X^{3k}+3X^{3k+1}-X^{3k+2}\big) \end{aligned}$$

3. Mealy machines

We will consider mappings

$$\begin{aligned} \mu[f] &: g(X) \mapsto f(X)g(X), \\ \alpha[f] &: g(X) \mapsto f(X)+g(X), \end{aligned}$$

where $f(X)$ and $g(X)$ are elements of ring $R[[X]]$.

We recall some facts from [6]. Details see in [2], [3] and [4].

3.1. Proposition.

- *$\alpha[f]$ is a bijection;*
- *if f is invertible in ring $R[[x]]$, then $\mu[f]$ is bijective;*
- *if f is invertible in ring $R[[x]]$, then $(\mu[f])^{-1}=\mu[f^{-1}]$;*
- *if f is invertible in ring $R[[x]]$, then $\mu[f^{-1}]\alpha[h]\mu[f]=\alpha[fh]$*

3.2. Definition. *Mapping*

$$\sigma(f)=\sum_{k=0}^{\infty}a_{k+1}X^k$$

is called a shift. Here $f(X)=\sum\limits_{k=0}^{\infty}a_kX^k$.

3.3. Corollary.

- *$f=a_0+\sigma(f)X$;*
- *$(1-aX)^{-1}=\sum\limits_{k=0}^{\infty}a^kX^k$;*
- *if $f=\dfrac{1}{1-aX}$ then $\sigma(f)=af$;*
- *if f is invertible in ring $R[[x]]$, then $\mu[f^{-1}]\alpha[h]\mu[f]=\alpha[fh]$*

3.4. Definition. *Let $\zeta : A^\omega \to B^\omega$ is ω–determined function. Function ζ defines set*

$$Q_\zeta=\{\zeta_u \mid u\in A^*\},$$

where ζ_u is restriction of function ζ. If set Q_f is finite, then ζ is called a finitely determined function.

3.5. Theorem. *If $f=\dfrac{1}{1-X}$, then $\mu[f]$ is finitely determined function, whose restriction set $Q_f=\{\mu[f]\circ\alpha[s] \mid s\in R\}$.*

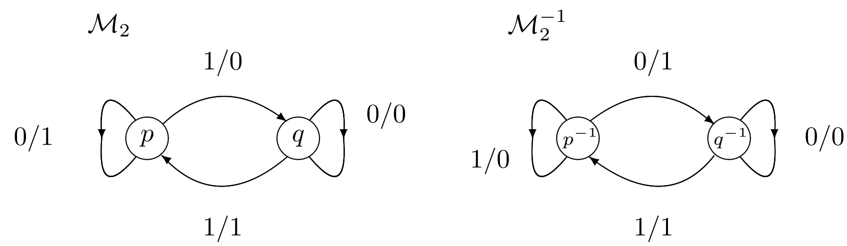
Let $f = \dfrac{1}{1-X}$. Define $\mathcal{M}_f = \langle Q_f, R, \circ, * \rangle$:

- with set $Q_f = \{\alpha[s]\mu[f] \mid s \in R\}$ of states and
- alphabet R,
- $Q \times R \xrightarrow{\circ} Q : \alpha[s]\mu[f] \circ r = \alpha[s+r]\mu[f]$,
- $Q \times A \xrightarrow{*} A : \alpha[s]\mu[f] * r = s + r$.

If R is Galois field $GF(2)$, then we obtain the Lamplighter group. Here

$$\alpha[0]\mu[f] \mapsto q, \qquad \alpha[1]\mu[f] \mapsto p$$

and $\Gamma(\mathcal{M}_2) = \langle \bar{q}, \bar{p} \rangle = \langle \alpha[0]\mu[f], \alpha[1]\mu[f] \rangle$.



1. Figure: Mealy machine generating the Lamplighter group.

Problem. Witch groups are generated by the rational series of commutative rings?

Here are some intuitive considerations as to why this might be interesting.

- Are all groups defined by rational formal power series of finite commutative rings infinite?
- If there still are finite groups defined by rational formal power series of finite commutative rings, then a question arises: is the finiteness problem algorithmically decidable?

3.6. Example. *What kind of group is determined by polynomial $f(X) = 1 + X + X^2$?*

Let $g(X) = s_0 + s_1X + s_2X^2 + \cdots = \sum_{k=0}^{\infty} s_kX^k$, then

$$\begin{aligned}
g\alpha[r]\mu[f] &= (r + s_0 + \sum_{k=1}^{\infty} s_kX^k)\mu[f] = (r+s_0)f(X) + f(X)\sum_{k=1}^{\infty} s_kX^k \\
&= (r+s_0) + (r+s_0)X + (r+s_0)X^2 \\
&+ (1 + X + X^2)(s_1X + s_2X^2 + s_3X^3 + s_4X^4 + \cdots) \\
&= (r+s_0) + (r+s_0)X + (r+s_0)X^2 \\
&+ s_1X + (s_1+s_2)X^2 \\
&+ (s_1+s_2+s_3)X^3 + (s_2+s_3+s_4)X^4 + (s_3+s_4+s_5)X^5 + \cdots \\
&= (r+s_0) + (r+s_0+s_1)X + (r+s_0+s_1+s_2)X^2 \\
&+ (s_1+s_2+s_3)X^3 + (s_2+s_3+s_4)X^4 + (s_3+s_4+s_5)X^5 + \cdots
\end{aligned}$$

$$
\begin{aligned}
g\mu[f] &= s_0 + (s_0+s_1)X + (s_0+s_1+s_2)X^2 + (s_1+s_2+s_3)X^3 + \cdots \\
&= s_0 + (s_0+s_1)X + \sum_{k=0}^{\infty}(s_k+s_{k+1}+s_{k+2})X^{k+2}.
\end{aligned}
$$

Hence

$$
\begin{aligned}
g\mu_r[f] &= r + s_0 + (r+s_0+s_1)X + (s_0+s_1+s_2)X^2 + (s_1+s_2+s_3)X^3 + \cdots \\
&= r + s_0 + (r+s_0+s_1)X + \sum_{k=0}^{\infty}(s_k+s_{k+1}+s_{k+2})X^{k+2},
\end{aligned}
$$

$$
\begin{aligned}
g\mu_{r^2}[f] &= 2r + s_0 + (r+s_0+s_1)X + (s_0+s_1+s_2)X^2 + (s_1+s_2+s_3)X^3 + \cdots \\
&= 2r + s_0 + (r+s_0+s_1)X + \sum_{k=0}^{\infty}(s_k+s_{k+1}+s_{k+2})X^{k+2},
\end{aligned}
$$

$$
\begin{aligned}
g\mu_{r^3}[f] &= 2r + s_0 + (r+s_0+s_1)X + (s_0+s_1+s_2)X^2 + (s_1+s_2+s_3)X^3 + \cdots \\
&= 2r + s_0 + (r+s_0+s_1)X + \sum_{k=0}^{\infty}(s_k+s_{k+1}+s_{k+2})X^{k+2},
\end{aligned}
$$

$$
g\mu_{r^n}[f] = 2r + s_0 + (r+s_0+s_1)X + \sum_{k=0}^{\infty}(s_k+s_{k+1}+s_{k+2})X^{k+2}.
$$

$$
\begin{aligned}
g\mu_{r_1r_2}[f] &= r_1 + r_2 + s_0 + (r_2+s_0+s_1)X + (s_0+s_1+s_2)X^2 + \cdots \\
&= r_1 + r_2 + s_0 + (r_2+s_0+s_1)X + \sum_{k=0}^{\infty}(s_k+s_{k+1}+s_{k+2})X^{k+2},
\end{aligned}
$$

$$
\begin{aligned}
g\mu_{r_1r_2r_3}[f] &= r_2 + r_3 + s_0 + (r_3+s_0+s_1)X + (s_0+s_1+s_2)X^2 + \cdots \\
&= r_2 + r_3 + s_0 + (r_3+s_0+s_1)X + \sum_{k=0}^{\infty}(s_k+s_{k+1}+s_{k+2})X^{k+2},
\end{aligned}
$$

$$
\begin{aligned}
g\mu_{r_1\cdots r_{n-1}r_n}[f] &= r_{n-1} + r_n + s_0 + (r_n+s_0+s_1)X + (s_0+s_1+s_2)X^2 + \cdots \\
&= r_{n-1} + r_n + s_0 + (r_n+s_0+s_1)X \\
&+ \sum_{k=0}^{\infty}(s_k+s_{k+1}+s_{k+2})X^{k+2},
\end{aligned}
$$

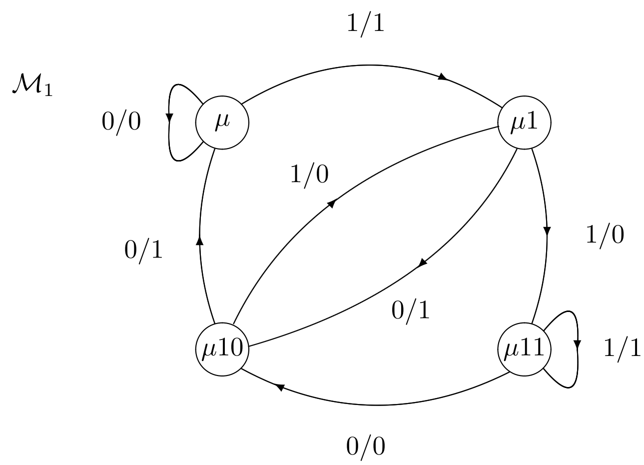
Lets introduce notation $\mu u \leftrightharpoons \mu_u[f]$ for each $u \in R^*$.

What happens if $R = GF(2)$?

from the above, it follows that:

$$
\begin{array}{lcr}
\mu = \mu 0 = \mu u00 & \dashrightarrow & s_0 + (s_0+s_1)X \\
\mu 1 = \mu 01 = \mu u01 & \dashrightarrow & 1 + s_0 + (1+s_0+s_1)X \\
\mu 10 = \mu u10 & \dashrightarrow & 1 + s_0 + (s_0+s_1)X \\
\mu 11 = \mu u11 & \dashrightarrow & s_0 + (1+s_0+s_1)X
\end{array}
$$

What happens if $R = GF(4)$?



2. Figure: Machine defined by $1 + X + X^2$ in field $GF(2)$.

addition $x+y$					multiplication xy			
$x \diagdown y$	0	1	a	b	0	1	a	b
0	0	1	a	b	0	0	0	0
1	1	0	b	a	0	1	a	b
a	a	b	0	1	0	a	b	1
b	b	a	1	0	0	b	1	a

$$
\begin{array}{lcr}
\mu = \mu 0 = \mu u 00 & \dashrightarrow & s_0 + (s_0 + s_1)X \\
\mu 1 = \mu 01 = \mu u 01 & \dashrightarrow & 1 + s_0 + (1 + s_0 + s_1)X \\
\mu a = \mu 0a = \mu u 0a & \dashrightarrow & a + s_0 + (a + s_0 + s_1)X \\
\mu b = \mu 0b = \mu u 0b & \dashrightarrow & b + s_0 + (b + s_0 + s_1)X \\
\mu 10 = \mu u 10 & \dashrightarrow & 1 + s_0 + (s_0 + s_1)X \\
\mu 11 = \mu u 11 & \dashrightarrow & s_0 + (1 + s_0 + s_1)X \\
\mu 1a = \mu u 1a & \dashrightarrow & b + s_0 + (a + s_0 + s_1)X \\
\mu 1b = \mu u 1b & \dashrightarrow & a + s_0 + (b + s_0 + s_1)X \\
\mu a0 = \mu u a0 & \dashrightarrow & a + s_0 + (s_0 + s_1)X \\
\mu a1 = \mu u a1 & \dashrightarrow & b + s_0 + (1 + s_0 + s_1)X \\
\mu aa = \mu u aa & \dashrightarrow & s_0 + (a + s_0 + s_1)X \\
\mu ab = \mu u ab & \dashrightarrow & 1 + s_0 + (b + s_0 + s_1)X \\
\mu b0 = \mu u b0 & \dashrightarrow & b + s_0 + (s_0 + s_1)X \\
\mu b1 = \mu u b1 & \dashrightarrow & a + s_0 + (1 + s_0 + s_1)X \\
\mu ba = \mu u ba & \dashrightarrow & 1 + s_0 + (a + s_0 + s_1)X \\
\mu bb = \mu u bb & \dashrightarrow & s_0 + (b + s_0 + s_1)X
\end{array}
$$

$\circ$	μ	$\mu 1$	μa	μb	$\mu 10$	$\mu 11$	$\mu 1a$	$\mu 1b$
0	μ	$\mu 10$	$\mu a0$	$\mu b0$	μ	$\mu 10$	$\mu a0$	$\mu b0$
1	$\mu 1$	$\mu 11$	$\mu a1$	$\mu b1$	$\mu 1$	$\mu 11$	$\mu a1$	$\mu b1$
a	μa	$\mu 1a$	μaa	μba	μa	$\mu 1a$	μaa	μba
b	μb	μ	μab	μbb	μb	$\mu 1b$	μab	μbb
$*$	μ	$\mu 1$	μa	μb	$\mu 10$	$\mu 11$	$\mu 1a$	$\mu 1b$
0	0	1	a	b	1	0	b	a
1	1	0	b	a	0	1	a	b
a	a	b	0	1	b	a	1	0
b	b	a	1	0	a	b	0	1

$\circ$	$\mu a0$	$\mu a1$	μaa	μab	$\mu b0$	$\mu b1$	μba	μbb
0	μ	$\mu 10$	$\mu a0$	$\mu b0$	μ	$\mu 10$	$\mu a0$	$\mu b0$
1	$\mu 1$	$\mu 11$	$\mu a1$	$\mu b1$	$\mu 1$	$\mu 11$	$\mu a1$	$\mu b1$
a	μa	$\mu 1a$	μaa	μba	μa	$\mu 1a$	μaa	μba
b	μb	$\mu 1b$	μab	μbb	μb	$\mu 1b$	μab	μbb
$*$	$\mu a0$	$\mu a1$	μaa	μab	$\mu b0$	$\mu b1$	μba	μbb
0	a	b	0	1	b	a	1	0
1	b	a	1	0	a	b	0	1
a	0	1	a	b	1	0	b	a
b	1	0	b	a	0	1	a	b

References

[1] Bini G., Flamini F. (2002) *Finite Commutative Rings and Their Applications.* Springer New York, 176 pages.

[2] Buls J., Užule L., Valainis A. (2018) *Automaton (Semi)groups (Basic Concepts).* https://arxiv.org/abs/1801.09552, 46 pages.

[3] Buls J. (2022) *The Lamplighter Group.* https://arxiv.org/abs/2202.04107, 29 pages.

[4] Eckenthal S. (2012) *The Lamplighter Group.* https://digitalrepository.trincoll.edu/cgi/viewcontent.cgi?article=1266&context=theses, 60 pages.

[5] Hou X–D., Lopez–Permouth S. R., Parra–Avila B. R. (2009) *Rational power series, sequential codes and periodicity of sequences.* Journal of Pure and Applied Algebra 213. P. 1157–1169.

[6] Skipper R., Steinberg B. (2019) *Lamplighter Groups, Bireversible Automata and Rational Series over Finite Rings.* https://arxiv.org/abs/1807.00433v3, 23 pages.