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 multi-
plicative 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 $R^*$. 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 $I$ of ring $R$ is called an ideal if
$RI \subseteq I$.

1.3. Proposition. If $I_1, I_2, \ldots, I_n$ are ideals of ring $R$, then mapping
$\Phi : R \rightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n : r \mapsto (r + I_1, r + I_2, \ldots, r + I_n)$
is a ring homomorphism.

□ We will use notation $[x]_j \equiv x + I_j$.
Let $x, y \in R$, then
$\Phi(x + y) = ([x + y]_1, [x + y]_2, \ldots, [x + y]_n)$
$= ([x]_1 + [y]_1, [x]_2 + [y]_2, \ldots, [x]_n + [y]_n)$
$= ([x]_1, [x]_2, \ldots, [x]_n) + ([y]_1, [y]_2, \ldots, [y]_n)$
$= \Phi(x) + \Phi(y)$
$\Phi(1) = ([1]_1, [1]_2, \ldots, [1]_n)$,
\[ \Phi(xy) = ([xy], [xy], \ldots, [xy]) \]
\[ = ([x][y], [x][y], \ldots, [x][y]) \]
\[ = (\langle x, y \rangle) \]
\[ = \Phi(x)\Phi(y). \]

1.4. Definition. \{0\} and \( R \) are called trivial ideals of ring \( R \).

All other ideals of ring \( R \) are called nontrivial ideals. Ideal \( I \) are called proper ideal if \( I \neq R \).

Let \( I_1, I_2, \ldots, I_n \) be proper ideals of ring \( R \).

1.5. Definition. Proper ideals \( I_k \) un \( I_m \), \( 1 \leq k < m \leq n \), are called coprime if \( I_k + I_m = R \).

Here \( I_k + I_m \equiv \{a + b \mid a \in I_k \land b \in I_m\} \)

1.6. Example. \( I_1 = \{0, 2, 4\} \), \( I_2 = \{0, 3\} \) are coprime ideals of ring \( \mathbb{Z}_6 \).

\[ I_1 \mathbb{Z}_6 = \{0, 2, 4\}\{0, 1, 2, 3, 4, 5\} = \{0, 2, 4\} \]
\[ 2 \cdot 3 = 6 \equiv 0 \quad 2 \cdot 4 = 8 \equiv 2 \quad 2 \cdot 5 = 10 \equiv 4 \]
\[ 4 \cdot 3 = 12 \equiv 0 \quad 4 \cdot 4 = 16 \equiv 4 \quad 4 \cdot 5 = 20 \equiv 2 \]
\[ I_2 \mathbb{Z}_6 = \{0, 3\}\{0, 1, 2, 3, 4, 5\} = \{0, 3\} \]
\[ 3 \cdot 3 = 9 \equiv 3 \quad 3 \cdot 4 = 12 \equiv 0 \quad 3 \cdot 5 = 15 \equiv 3 \]
\[ I_1 + I_2 = \{0, 2, 4\} + \{0, 3\} = \{0, 0, 0, 3, 2 + 0, 2 + 3, 4 + 0, 4 + 3\} = \{0, 3, 2, 5, 4, 7 \equiv 1\} = \mathbb{Z}_6 \]

Notice that
\[ \forall x \in I_1 \forall y \in I_2 \ xy = 0. \]

1.7. Proposition. If \( I_1, I_2, \ldots, I_n \) are coprime ideals of ring \( R \), then
\[ \bigcap_{k=1}^{n} I_k = \bigcap_{k=1}^{n} I_k \]

Notice that
\[ \prod_{k=1}^{n} I_k \equiv \{\sum_{k} x_{k1}x_{k2} \ldots x_{kn} \mid \forall j \ x_{kj} \in I_j\}. \]

Here, \( \sum_{k} x_{k1}x_{k2} \ldots x_{kn} \) denotes all possible finite sums of such form. In sum \( \sum_{k} x_{ky} \) there is a possibility for \( x_1 = x_2 \), but if so then \( y_1 \neq y_2 \).

As \( I_1 \) un \( I_2 \) are ideals, then
\[ I_1 \cap I_2 = \{h \in R \mid h \in I_1 \land h \in I_2\} \]
is a proper ideal since \( 0 \in I_1 \cap I_2 \). Notice that
\[ \prod_{k=1}^{2} I_k = I_1I_2 = \{\sum_{k} x_{ky} \mid x_{k} \in I_1 \land y_{k} \in I_2\}. \]
Each member of sum \( \sum_k x_k y_k \) belongs to ideal \( \mathcal{I}_1 \) 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 \( \mathcal{I}_1 \mathcal{I}_2 = \mathcal{I}_1 \mathcal{I}_2 \).

Notice that \( \prod_{k=1}^n \mathcal{I}_k = \{ \sum_k x_k y_k \mid \forall j \ x_{kj} \in \mathcal{I}_j \} \). As the ring is commutative, it follows that each member of \( \sum_k x_k y_k \) is a member of an arbitrary ideal \( \mathcal{I}_k \), \( k \in \{1, \ldots, n\} \), therefore \( \prod_{k=1}^n \mathcal{I}_k \subseteq \bigcap_{k=1}^n \mathcal{I}_k \).

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

\[
\bigcap_{k=1}^{m+1} \mathcal{I}_k = \left( \bigcap_{k=1}^m \mathcal{I}_k \right) \cap \mathcal{I}_{m+1} = \left( \prod_{k=1}^m \mathcal{I}_k \right) \cap \mathcal{I}_{m+1}
\]

As all the pairs \( \mathcal{I}_{m+1}, \mathcal{I}_k, k \in \{1, \ldots, m\} \) 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

\[
1 = (a_1 + b_1)(a_2 + b_2) \cdots (a_m + b_m) = a_1 a_2 \cdots a_m + B,
\]

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 \( a \in \bigcap_{k=1}^{m+1} \mathcal{I}_k \), then

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

As \( a \in \bigcap_{k=1}^{m+1} \mathcal{I}_k \), it follows that \( a \in \bigcap_{k=1}^m \mathcal{I}_k \).

From the inductive assumption \( \bigcap_{k=1}^m \mathcal{I}_k = \prod_{k=1}^m \mathcal{I}_k \). Therefore \( a \) can be written as a sum \( \sum_k x_k y_k \), where \( \forall x_{kj} \in \mathcal{I}_j \). Thus

\[
aB = \sum_k x_k y_k B \in \prod_{k=1}^{m+1} \mathcal{I}_k,
\]

and therefore

\[
a = a_1 a_2 \cdots a_m a + aB = a_1 a_2 \cdots a_m a + \sum_k x_k y_k B \in \prod_{k=1}^{m+1} \mathcal{I}_k.
\]

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 \( \mathcal{I}^m = \mathcal{I} \cdots \mathcal{I} \).

\[\square \] 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 \( a^2 + b^2 \in I^2 + J^2 \);
• If \( ab \neq 0 \), then \( 2ab = 1 \cdot 2ab = 2(a + b)ab = 2a^2b + 2ab^2 \in I^2 + J^2 \).

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

\[ 1 = (a + b)^2 = a^2 + 2ab + b^2. \]

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

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

\[ a = \sum_i x_{i1}x_{i2}x_{i3}\ldots x_{im+1} = \sum_i(x_{i1}x_{i2})x_{i3}\ldots x_{im+1} \in I^m, \]

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


1.9. Proposition. Ring homomorphism \( f : G \to G' \) is monomorphism if and only if \( \text{Ker} f = 0 \).

\( \Box \Rightarrow \) 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 \( \text{Ker} f = 0 \), then \( x - y = 0 \), i.e., \( x = y \). ■

1.10. Proposition. Assume that \( I_1, I_2,\ldots, I_n \) are ideals of ring \( R \). Mapping

\[ \Phi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n : r \mapsto (r + I_1, r + I_2,\ldots, r + I_n) \]

is ring monomorphism if and only if \( \bigcap_{k=1}^n I_k = 0 \).

\( \Box \) Let \( \Phi(r) = ([0], [0],\ldots, [0]) \). Therefore \( r \in \bigcap_{k=1}^n I_k \). It shows that \( \text{Ker} \Phi = \bigcap_{k=1}^n I_k \). From previous proposition follows that \( \Phi \) is injective only when \( \text{Ker} \Phi = 0 \), i.e., \( 0 = \text{Ker} \Phi = \bigcap_{k=1}^n I_k \). ■

1.11. Lemma. If \( I_1, I_2,\ldots, I_n \) are coprime ideals of ring \( R \), then \( I_1 \) and \( \prod_{k=2}^n I_k \) are coprime ideals of ring \( R \).

\( \Box \) We have (1.7. Proposition) \( \prod_{k=2}^n I_k = \prod_{k=2}^n I_k \), therefore \( \prod_{k=2}^n I_k \) is an ideal. As all pairs \( I_1, I_k, k \in \{1, n\} \) are coprime, then there exist such \( a_k \in I_1, b_k \in I_k \), 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 multiplier, therefore \( A \in I_1 \).

Thus \( 1 = A + b_2b_3\cdots b_n \), where \( A \in I_1 \) and \( b_2b_3\cdots b_n \in \prod_{k=2}^n I_k \). ■
1.12. Proposition. Assume that $I_1, I_2, \ldots, I_n$ are ideals of ring $R$.

Mapping

$\Phi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n : r \mapsto (r + I_1, r + I_2, \ldots, r + I_n)$

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

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

$\Phi(x) = ([1], [0], \ldots, [0]).$

$\Phi(1 - x) = \Phi(1) - \Phi(x)$

$= ([1], [1], \ldots, [1]) - ([1], [0], \ldots, [0])$

$= ([0], [1], \ldots, [1])$

It shows that $1 - x \in I_1$, and also $x \in I_k$ for all $k \in \overline{2, n}$. Hence $1 \in I_1 + I_k$ for all $k \in \overline{2, n}$.

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

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

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

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

It shows that $1 - x_m \in I_m$. Also $x_m \in I_k$ for all $k \neq m$. Hence $1 \in I_m + I_k$ for all $k \neq m$.

$\Leftarrow$ Assume that all pairs $I_k, I_j$ of ideals are coprime.

If $n = 2$, then there exist such $x \in I_1, y \in I_2$, that $x + y = 1$. As $x = 1 - y$ and $y = 1 - x$, then

$[x]_2 = [1 - y]_2 = [1]_2 - [y]_2 = [1]_2 - [0] = [1]_2,$

$[y]_1 = [1 - x]_1 = [1]_1 - [x]_1 = [1]_1,$

$\Phi(x) = ([x]_1, [x]_2) = ([0]_1, [1]_2),$

$\Phi(y) = ([y]_1, [y]_2) = ([1]_1, [0]_2),$

$\Phi(bx + ay) = \Phi(b)\Phi(x) + \Phi(a)\Phi(y)$

$= ([b]_1, [b]_2)([0]_1, [1]_2) + ([a]_1, [a]_2)([1]_1, [0]_2)$

$= ([0]_1, [b]_2) + ([a]_1, [0]_2) = ([a]_1, [b]_2).$

Hence mapping $\Phi$ is surjective. Further proof is inductive.

From (1.1.4. Lemma) follows, that $I_1, I_2I_3 \cdots I_n$ are coprime, therefore homomorphism

$\Psi : R \to R/I_1 \times R/I_2I_3 \cdots I_n : r \mapsto (r + I_1, r + I_2I_3 \cdots I_n)$

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

$\Phi_2 : R \to R/I_2 \times R/I_3 \cdots R/I_n : r \mapsto (r + I_2, r + I_3, \ldots, r + I_n)$
ir surjective. From the homomorphism theorem, there exists such homomorphism $\Phi_2$, that diagram

$$
\begin{array}{ccc}
R & \xrightarrow{\Phi_2} & R/I_2 \times R/I_3 \times \cdots \times R/I_n \\
\pi & & \Phi_2^* \\
R/Ker\Phi_2 & \end{array}
$$

is commutative. Additionally, homomorphism $\Phi_2^*$ is a monomorphism. Therefore $R/Ker\Phi_2$ is isomorphic with ring $R/I_2 \times R/I_3 \times \cdots \times R/I_n$ (homomorphism $\Phi_2$ is also surjective).

From proof of (1.10. Proposition) follows, that $\text{Ker}\Phi_2 = \bigcap_{k=2}^n I_k$, additionally (1.7. Proposition) $\bigcap_{k=2}^n I_k = \bigcap_{k=2}^n I_k$. Therefore $R/I_2 I_3 \cdots I_n$ is isomorphic with $R/I_2 \times R/I_3 \times \cdots \times R/I_n$.

Hence mapping $\Phi_2 : R/I_2 I_3 \cdots I_n \rightarrow R/I_2 \times R/I_3 \times \cdots \times R/I_n$ is an isomorphism.

Let $([r_1], [r_2], \ldots, [r_n]) \in R/I_1 \times R/I_2 \times R/I_3 \times \cdots \times R/I_n$. Notice that

$$
\begin{align*}
\Phi_1 : r & \mapsto ([r_1], [r_2], \ldots, [r_n]), \\
\Phi_2 : r & \mapsto ([r_2], [r_3], \ldots, [r_n]).
\end{align*}
$$

From the inductions assumption, mapping $\Phi_2$ is an epimorphism, therefore there exists such $x \in R$, that

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

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

$$
\Psi : r \mapsto (r + I_1, r + I_2 I_3 \ldots I_n).
$$

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

$$
\Psi : y \mapsto (y + I_1, y + I_2 I_3 \ldots I_n),
$$

where $y + I_1 = [y]_1 = [r_1]$ and $(\Phi_2^*)^{-1}([r_2], [r_3], \ldots, [r_n]) = y + I_2 I_3 \ldots I_n$. Notice that $[y]_1 = [r_1]$, thus

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

Diagram (D) is commutative, therefore

$$
\begin{align*}
([y]_2, [y]_3, \ldots, [y]_n) & = \Phi_2(y) = \Phi_2^*(\pi(y)) = \Phi_2^*(y + I_2 I_3 \ldots I_n) \\
& = ([r_2], [r_3], \ldots, [r_n]).
\end{align*}
$$

Thus $\Phi_1 : y \mapsto ([r_1], [r_2], \ldots, [r_n])$, showing that mapping $\Phi_1$ 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 \( \sum_{i=1}^{n} e_i = 1 \) and \( R_i \cong e_iR \);
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 \( \mathcal{I}_j \cong R_j \).

\( 1 \Rightarrow 2 \). 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 \( \varphi(e_k) \mapsto e_k \) 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
\[
1 = \varphi(1,1,\ldots,1) = \varphi\left( \sum_{k=1}^{n} \delta_k \right) = \sum_{k=1}^{n} \varphi(\delta_k) = \sum_{k=1}^{n} e_k.
\]
\[
\varphi^{-1}(e_k e_i) = \varphi^{-1}(e_k)\varphi^{-1}(e_i) = (0,0,\ldots,0) \quad \text{if } i \neq k.
\]
As \( \varphi \) 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 \( x_j \in R_j \).
\[
\varphi^{-1}(e_i x) = \varphi^{-1}(e_i)\varphi^{-1}(x) = (0,0,\ldots,1,0)(x_1, x_2, \ldots, x_i, \ldots, x_n) = (0,0,\ldots,x_i,0).
\]

Hence \( e_i R \cong R_i \).

2. \( \Rightarrow 3 \). \( \mathcal{I}_j \subseteq e_j R \). 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 \( \vec{a} = (a_1, a_2, \ldots, a_n) \in \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n \) and \( \vec{b} = (b_1, b_2, \ldots, b_n) \in \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n \), then
\[
\varphi(\vec{a} + \vec{b}) = \varphi(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = a_1 + b_1 + a_2 + b_2 + \cdots + a_n + b_n = (a_1 + a_2 + \cdots + a_n) + (b_1 + b_2 + \cdots + b_n) = \varphi(\vec{a}) + \varphi(\vec{b}).
\]
(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 \( xy = e_j x' e_k y' = e_j e_k x' y' = 0x'y' = 0 \).

\[
\varphi(ab) = \varphi((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)) = \varphi(a_1b_1, a_2b_2, \ldots, a_nb_n) = a_1b_1 + a_2b_2 + \cdots + a_nb_n = (a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) = \varphi(a)\varphi(b).
\]

(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

\[
x = e_j x_j = e_k x_k = 0 \cdot x_k = 0.
\]

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 \( \varphi(a) = \varphi(b) \), 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

\[
e_i(x_i - y_i) = \sum_{j \neq i} e_j(y_j - x_j),
e_i(x_i - y_i) = e_i^2(x_i - y_i) = \sum_{j \neq i} e_i e_j(y_j - x_j) = 0.
\]

Then \( a_i - b_i = e_i x_i - e_i y_i = 0 \) or \( a_i = b_i \). We have proven that \( \varphi \) 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

\[
(x_1, x_2, \ldots, x_n) \in \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n,
x_1 + x_2 + \cdots + x_n = e_1 x + e_2 x + \cdots + e_n x
\]

\[
= (e_1 + e_2 + \cdots + e_n)x = 1 \cdot x = x.
\]

Hence \( \varphi(x_1, x_2, \ldots, x_n) = x \). Therefore \( \varphi \) is surjective. We can conclude that \( \varphi \) 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. \( \blacksquare \)

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

\[
ab \in \mathcal{I} \Rightarrow a \in \mathcal{I} \lor b \in \mathcal{I}.
\]
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 $R$:

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

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

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

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

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.

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: $[1] = [u + yx] = [u] + [yx] = [0] + [y][x] = [y][x]$. ■

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

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

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 $R$.

As $R/\mathcal{M}$ is a field, then card($R/\mathcal{M}$) $\geq 2$. Let $\mathcal{M} \neq R$. If $\mathcal{I}$ is an ideal such that $\mathcal{M} \subseteq \mathcal{I} \subseteq R$, 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 $\mathcal{M} \subseteq \mathcal{I}$, 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 $\mathcal{I} = R$. ■

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

1.23. Corollary. $\text{Specm}(R) \subseteq \text{Spec}(R)$.

1.24. Definition. Jacobson radical:

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

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.

\[ \Rightarrow [a][b] = [0] \Rightarrow ab \in I. \]

Thus \([a] = [0] \lor [b] = [0]\). Hence \(R/I\) is an integral domain.

\[ \Leftarrow \]

Assume that \(I\) is not prime, then exist such \(a \notin I\) and \(b \notin I\), that \(ab \in I\). \([a][b] = [0] \in R/I\) and \([a] \neq [0] \land [b] \neq [0]\). Hence \(R/I\) is not an integral domain.

\[ \Box \]

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

\[ \Box \]

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 \(I\) is a prime ideal of ring \(R\), then it is a maximal ideal.

\[ \Box \]

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

1.28. Proposition. If \(I\) and \(J\) are distinct maximal ideals of ring \(R\), then they are coprime ideals.

\[ \Box \]

As \(I \neq J\), then \(I + J \supset I\) or \(I + J \supset J\). Thus \(R \supset I + J \supset I\) or \(R \supset I + J \supset J\).

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

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 \(\text{Nil}(R)\), consisting of all nilpotent elements of ring \(R\), is called a nilradical.

1.31. Proposition. \(\text{Nil}(R)\) is ideal of ring \(R\).

\[ \Box \]

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 \(R \text{Nil}(R) \subseteq \text{Nil}(R)\).
1.32. Proposition. If $R$ is a commutative ring, then

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

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

Let's now assume that $f \not\in \text{Nil}(R)$ and consider set

$$\mathfrak{J} = \left\{ J \subseteq R \mid J \text{ is an ideal and } \forall m \in \mathbb{Z}_+ f^m \not\in J \right\}.$$ 

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

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

Let's prove that $\exists$ is an ideal.

If $a, b \in \exists$, then $\exists a, b \in J_k$. Assume for concreteness that $J_i \subseteq J_k$, then $a \in J_k$. Hence $a + b \in J_k \subseteq \exists$.

Let $r \in R$ un $c \in \exists$, then $\exists c \in J_k$. Hence $rc \in J_k \subseteq \exists$. A contradiction!

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

Let $a \not\in \mathcal{M}$ and $b \not\in \mathcal{M}$, then $aR + \mathcal{M} \supset \mathcal{M}$ and $bR + \mathcal{M} \supset \mathcal{M}$. Therefore $aR + \mathcal{M} \not\in \exists$ and $bR + \mathcal{M} \not\in \exists$, thus

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

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 $m_2 \in \mathcal{M}$.

$$f^{n+m} = f^n f^m = (ar_1 + m_1)(br_2 + m_2) = abr_1 r_2 + ar_1 m_2 + br_2 m_1 + m_1 m_2.$$ 

Hence $f^{n+m} \in abR + \mathcal{M}$. Therefore $abR + \mathcal{M} \not\in \exists$, thus $ab \not\in \mathcal{M}$.

With some logical transformations:

$$a \not\in \mathcal{M} \land b \not\in \mathcal{M} \Rightarrow ab \not\in \mathcal{M},$$ 

$$-(a \not\in \mathcal{M} \land b \not\in \mathcal{M}) \lor (ab \not\in \mathcal{M}),$$ 

$$a \in \mathcal{M} \lor b \in \mathcal{M} \lor (ab \not\in \mathcal{M}),$$ 

$$ab \not\in \mathcal{M} \lor a \in \mathcal{M} \lor b \in \mathcal{M},$$ 

$$ab \in \mathcal{M} \Rightarrow a \in \mathcal{M} \lor b \in \mathcal{M}.$$ 

Therefore $\mathcal{M}$ is a prime ideal. A contradiction!

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

$$f \not\in \text{Nil}(R) \Rightarrow \exists \mathcal{M} \in \text{Spec}(R) \ (f \not\in \mathcal{M}).$$
From contraposition, we obtain:

\[ \forall M \in \text{Spec}(R) \ (f \in M) \Rightarrow f \in \text{Nil}(R). \]

That proves the inclusion \( \bigcap_{I \in \text{Spec}(R)} I \subseteq \text{Nil}(R). \) ■

**1.33. Lemma.** There exists \( m \), that \( (\text{Nil}(R))^m = 0. \)

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

\[ \kappa = \max_{a \in \text{Nil}(R)} (\kappa_a). \]

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

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

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

\[ a' x' = \phi(a) \phi(x) = \phi(ax) \in \phi(I). \]

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

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

(i) Let’s define

\[ I \leftarrow \{ x \in G | \exists x' \in I' \phi(x) = x' \}. \]

(ii) Let \( a \in I \) un \( b \in I \), then

\[ \phi(a + b) = \phi(a) + \phi(b) \in I', \]

\[ \phi(ab) = \phi(a)\phi(b) \in I'. \]

Thus \( a + b \) and \( ab \) belong to set \( I \).

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

Let us consider groups. A subgroup, as usual, is denoted by \( \leq \), and a normal subgroup is denoted by \( \triangleleft \).

**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 \( K \):

\[ K = \{ hN | hN \in K \land h \in G \}. \]

Let’s define \( H \leftarrow \{ h | hN \in H \land h \in G \}. \) Thus \( h \in H \iff hN \in H \). 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 \( K \subseteq G/N \), 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 \( H \subseteq G \).

(iii) Notice
\[
H/N = \{hN \mid h \in H\} = \{hN \mid hN \in K\} = K. \quad \blacksquare
\]

1.37. Theorem (Correspondence theorem). Let \( N \subseteq G \).

(i) If \( N \subseteq H \subseteq G \), then \( H/N \subseteq G/N \).

(ii) If \( K \subseteq G/N \), then there exist such \( H \subseteq G \), that \( K = H/N \).

(iii) Let
\[
\begin{align*}
S &= \{H \mid N \subseteq H \land H \subseteq G\}, \\
\mathcal{J} &= \{K \mid K \subseteq G/N\}.
\end{align*}
\]

If \( \phi : S \to G/N : H \mapsto H/N \), then \( \phi : S \to \mathcal{J} \) is a bijection.

\( \square \) (i) Let \( gN \in G/N \) un \( hN \in H/N \), then
\[
(gN)(hN)(gN)^{-1} = (ghN)(g^{-1}N) = ghg^{-1}N.
\]

As \( H \subseteq G \), 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 \( H/N \subseteq G/N \).

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

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 \( H/N \subseteq G/N \), 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 \( H \subseteq G \).

(iii) From (ii) for each element \( K \) of set \( \mathcal{J} \) there exists such \( H \subseteq G \), that \( K = H/N \). Thus range of \( \phi : S \to G/N : H \mapsto H/N \) is \( \text{Ran}(\phi) = \mathcal{J} \), and thus mapping \( \phi : S \to \mathcal{J} \) is surjective (with \( \mathcal{J} \) 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 \( \phi : S \to \mathcal{J} \) is an injection. \( \blacksquare \)

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

1.38. Theorem (Correspondence theorem for rings). Assume that
\[
\begin{align*}
\bullet & \quad R \text{ is a ring;} \\
\bullet & \quad I \subseteq R \text{ is an ideal;}
\end{align*}
\]
\begin{itemize}
  \item \( \pi : R \to R/I : r \mapsto [r] \) is the natural mapping;
  \item \( S = \{ G \mid I \subseteq G \text{ and } G \text{ is a subring of } R \} \);
  \item \( \mathcal{S} = \{ H \mid H \text{ is a subring of ring } R/I \} \).
\end{itemize}

Mapping \( \phi : S \to \mathcal{S} : G \mapsto G/I \) is a bijection. If
\begin{itemize}
  \item \( S' = \{ J \mid I \subseteq J \text{ and } J \text{ is an ideal of } R \} \),
  \item \( \mathcal{S}' = \{ L \mid L \text{ is an ideal of ring } R/I \} \),
\end{itemize}
then mapping \( \psi : S' \to \mathcal{S}' : J \mapsto J/I \) is a bijection.

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

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

Let \( H \) be a subring of ring \( R/I \), then for \( H \) the additive group can be expressed as (1.37. Theorem) \( H = A/I \), where \( A \) is a subgroup of the additive group of ring \( R \). Thus \( a \in A \iff a + I \in A/I \). As \( H = A/I \) is a subring, then \((a + I)(b + I) = ab + I \) 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 \( \phi \), we have \( \phi(A) = A/I \). Thus mapping \( \phi \) is surjective.

(ii) Let \( L \) be an ideal of ring \( R/I \), than the additive group of \( L \) can be expressed (1.37. Theorem) as \( L = A/I \), where \( A \) is a subgroup of the additive group of ring \( R \). Thus \( a \in A \iff a + I \in A/I \). As \( L = A/I \) is an ideal, then \( ra + I = (r + I)(a + I) \in A/I \) 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 \( \psi \) we have \( \psi(A) = A/I \). Hence mapping \( \psi \) is surjective.

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

We must prove that \( J/I \) is an ideal. From the definition of \( J/I \) follows, that \( a \in J \iff a + I \in J/I \). If \( r \in R \), then \( ar \in J \), thus \( (a + I)(r + I) = ar + I \in J/I \).

Therefore \( J/I \) is ideal of ring \( R/I \). Hence mapping \( \psi \) is also injective. \( \blacksquare \)

1.39. Corollary. Assume that
\begin{itemize}
  \item \( R \) is a ring;
  \item \( I \subseteq R \) is an ideal;
  \item \( \pi : R \to R/I : r \mapsto [r] \) is the natural mapping;
  \item \( S' = \{ J \mid I \subseteq J \text{ and } J \text{ is an ideal of } R \} \);
  \item \( \mathcal{S}' = \{ L \mid L \text{ is an ideal of ring } R/I \} \);
  \item \( \psi : S' \to \mathcal{S}' : J \mapsto J/I \).
\end{itemize}

\( J/I \) is a maximal ideal of ring \( R/I \) if and only if \( J \) is a maximal ideal of ring \( R \), and \( J \) contains ideal \( I \).
Notice that mapping $\psi$ is bijective.

$\Rightarrow$ Assume that $L$ is a maximal ideal if ring $R/I$. We already know that there exist an ideal $\mathcal{J}$ of ring $\mathcal{R}$, $I \subseteq \mathcal{J}$, that $L = \mathcal{J}/I$ and $\psi(\mathcal{J}) = \mathcal{J}/I$.

If in turn, $\mathcal{J}$ is not a maximal ideal, then there exists such ideal $\mathfrak{M}$ of ring $\mathcal{R}$, that $\mathcal{J} \subseteq \mathfrak{M} \subseteq R$. Thus if $\mathcal{J} \subseteq \mathfrak{M}$, then $\mathcal{J}/I \subseteq \mathfrak{M}/I$. As $\psi$ is bijective, then $\mathcal{J}/I \neq \mathfrak{M}/I$. Thus $\mathcal{J}/I \subseteq \mathfrak{M}/I$, e.i., $\mathcal{J}/I$ is not a maximal ideal. A contradiction!

$\Leftarrow$ Assume that $J$ is a maximal ideal of ring $R$, $I \subseteq J$. If in turn, $J/I$ is not a maximal ideal of ring $R/I$, then there exists such ideal $M$ of ring $R/I$, that $J/I \subseteq M/I \subseteq R/I$. Thus if $J/I \subseteq M/I$, then $J/I \subseteq M/I$. As $\psi$ is bijective, then $J/I \neq M/I$. Thus $J/I$ is not a maximal ideal. A contradiction!

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

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

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

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

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

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

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

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

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

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

(ii) Let

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

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

15
Let \( b \in \mathcal{J} \) and \( c \in \mathcal{J} \). Then there exist such \( \beta \) and \( \gamma \), that \( b \in \mathcal{J}_\beta \) and \( c \in \mathcal{J}_\gamma \). We have \( \mathcal{J}_\beta \subset \mathcal{J} \), or \( \mathcal{J}_\gamma \subset \mathcal{J} \). For concreteness assume \( \mathcal{J}_\beta \subset \mathcal{J} \), then \( b \) and \( c \) are elements of ideal \( \mathcal{J} \). As \( \mathcal{J} \) is an ideal, then \( b + c \in \mathcal{J} \), also \( 0 \in \mathcal{J} \) and \(-b \in \mathcal{J} \). As \( \mathcal{J} \) is an ideal, then \( br \in \mathcal{J}_r \) 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 \( \mathcal{J} \in \mathcal{S} \) and is upper bound of chain \( \{ \mathcal{J}_\alpha \} \). According to Zorn’s lemma, set \( \mathcal{S} \) has at least one maximal element \( \mathfrak{M} \). Thus \( \mathfrak{M} \) is a maximal ideal and \( \mathfrak{M} \neq \mathfrak{M}_e \), because \( a \notin \mathfrak{M} \) and \( a \notin \mathfrak{M} \). 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.

\( \square \) 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 \( e \).

\( \square \) 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 \( xe = x \), where \( r \in R \).

\[ xe = ex = e^2r = er = x. \square \]

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

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

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

Additionally, if \( k \neq x \), then ideals \( P_k \) and \( P_x \) 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 \( x_{kj} = \sum \gamma_{kj1} \gamma_{kj2} \ldots \gamma_{kjn} \gamma_{kj}, \) where all \( \gamma_{kj} \in P_j \). 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

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

Let’s define a homeomorphism of rings

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

Homeomorphism $\Phi$ is injective (1.10. Proposition), because

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

Additionally $\Phi$ is surjective (1.12. Proposition), because $P_i^m$, $P_j^m$ are coprime, if $i \neq j$. Thus $\Phi$ 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 $R = P_k^m + P_l^m \subseteq P_l + P_i^m \subseteq P_l = P_l$. A contradiction!

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

\[ e_j = e_j \sum_{k=1}^m f_k = \sum_{k=1}^m e_j f_k \in e_j R, \]

\[ (e_j f_k)^2 = e_j f_k. \]

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

\[ e_j f_k = 0, \text{ vai } e_j f_k = e_j. \]

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 $\kappa$, 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
\[ \{e_1, e_2, \ldots, e_n\} = \{f_1, f_2, \ldots, f_n\}. \]

2. Periodical rings

We are following [5] in this section.
Assume \( X \not\in R \). We identify set \( R^\omega \) with \( R[[X]] \), i.e., by using standard notation
\[ a_0 a_1 a_2 \cdots a_n \cdots \rightarrow \sum_{k=0}^{\infty} a_k X^k. \]
If \( f = \sum_{k=0}^{\infty} a_k X^k \), then we use notation for coefficient extraction \( f(n) = a_n \).

2.1. Definition. Algebra \( \langle R[[X]], +, \cdot \rangle \) is called formal power series if
\[ \sum_{k=0}^{\infty} a_k X^k + \sum_{k=0}^{\infty} b_k X^k = \sum_{k=0}^{\infty} (a_k + b_k) X^k, \]
\[ \left( \sum_{k=0}^{\infty} a_k X^k \right) \left( \sum_{k=0}^{\infty} b_k X^k \right) = \sum_{k=0}^{\infty} \left( \sum_{i=0}^{k} a_i b_{k-i} \right) X^k. \]

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

2.2. Proposition. Series \( f = \sum_{k=0}^{\infty} a_k X^k \) 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 \( A = a_0 + a_1 X + \ldots \) has a multiplicative inverse \( B = b_0 + b_1 X + \ldots \), 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:
\[ b_0 = a_0^{-1}; \quad b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-i}, \quad n \geq 1. \]

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 \( f = \sum_{i=0}^{\infty} a_i X^i \) is called periodical series if there exists such \( k \in \mathbb{Z}_+ = \{1, 2, \ldots, n, \ldots\} \), that \( \forall i a_{i+k} = a_i \). Series \( f \) is called semiperiodic series, if there exist such \( n \in \mathbb{Z}_+ \), that series \( \sum_{j=0}^{n} a_{j+n} X^j \) is periodical.
2.5. Proposition. If series \( f \in R[[X]] \) is semiperiodic series, then series \( f \) is rational series.

\[ f = a_0 + a_1 X + \ldots + a_m X^m + \sum_{i=0}^{\infty} (a_{m+i+1} X^{m+i+1} + a_{m+i+2} X^{m+i+2} + \ldots + a_{m+i+n} X^{m+i+n}) X^{in} \]

\[ = p(X) + q(X) \sum_{i=0}^{\infty} X^{in} \]

\[ = p(X) + \frac{q(X)}{1-X^n}. \]

Here

\[ p(X) = a_0 + a_1 X + \ldots + a_m X^m, \]
\[ q(X) = a_{m+1} X^{m+1} + a_{m+2} X^{m+2} + \ldots + a_{m+n} X^{m+n}. \]

2.6. Definition. Ring \( R \) is called a periodic ring, if

\[ \forall a \in R \exists m \in \mathbb{Z}_+ \exists n \in \mathbb{Z}_+ (m \neq n \land a^m = a^n). \]

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

\[ \lambda : \mathbb{Z} \rightarrow R : k \mapsto k1. \]

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

Let \( e \) be the unit element of periodic ring \( R \). If \( e \neq 0 \) and \( e + e = 0 \), then \( \text{char}(R) = 2 \). 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 \( (e + e)^m + (e + e)^n = 0 \), i.e.,

\[ 0 = (e + e)^m + (e + e)^n \]
\[ = \sum_{i=0}^{m+n} \binom{m+n}{i} e - \sum_{i=0}^{n} \binom{n}{i} e \]
\[ = \left( \sum_{i=0}^{m+n} \binom{m+n}{i} - \sum_{i=0}^{n} \binom{n}{i} \right) e. \]

Here \( ke = e + e + \cdots + e \). Note that \( 2e \) is not idempotent. If the contrary is true, then \( e + e = (e + e)^2 = e^2 + e^2 = e + 2e + e \). Hence \( e + e = 0 \).

2.9. Proposition. If \( \text{char}(R) = m \neq 0 \), then there exist such subring \( G \) of ring \( R \), that \( G \) is isomorph to ring \( \mathbb{Z}_m \).
Let’s define set \( G \rightleftharpoons \{ke \mid k \in \mathbb{N}\} \), here \( e \) is the unit element of ring \( R \). If
\[
    k + n = mq_1 + r_1, \quad 0 \leq r_1 < m;
    \quad kn = mq_2 + r_2, \quad 0 \leq r_2 < m,
\]
then
\[
    (k + n)e = (mq_1 + r_1)e = q_1(me) + r_1e = r_1e,
    \quad kn = (mq_2 + r_2)e = q_2(me) + r_2e = r_2e.
\]
In \( \mathbb{Z}_m \) we have
\[
k + n \equiv r_1 \mod m,
    \quad kn \equiv r_2 \mod m.
\]
Hence mapping \( f : G \rightarrow \mathbb{Z}_m : ke \mapsto k \) 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 isomorphic 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
\[
f : R/\mathcal{I} \rightarrow R/\mathcal{J} : x + \mathcal{I} \mapsto x + \mathcal{J}
\]
is an epimorphism of rings.

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:
\[
    [x]_\mathcal{I} \rightleftharpoons x + \mathcal{I},
    \quad [x]_\mathcal{J} \rightleftharpoons x + \mathcal{J},
\]
then
\[
f[x + y]_\mathcal{J} = [x + y]_\mathcal{J} = [x]_\mathcal{J} + [y]_\mathcal{J} = f[x]_\mathcal{I} + f[y]_\mathcal{I},
    \quad f[xy]_\mathcal{J} = [xy]_\mathcal{J} = [x]_\mathcal{J}[y]_\mathcal{J} = f[x]_\mathcal{I}[f[y]_\mathcal{I},
    \quad f[1]_\mathcal{J} = [1]_\mathcal{J}.
\]
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 \( f[x]_\mathcal{J} = [x]_\mathcal{J} \), 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 \( |R[X]/(g(X))| < \infty \).

\( \Box \) (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) \( a_{t+1}, a_{t+2}, \ldots, a_k \notin \mathfrak{M} \).

(ii) Maximal ideal \( \mathfrak{M} \) of ring \( R \) is prime (1.20. Corollary). If \( I \) 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) 
\[ \text{Nil}(R) = \bigcap_{\mathcal{I} \in \text{Spec}(R)} \mathcal{I}. \]

Here
- \( \text{Nil}(R) \) is a nilradical, e.i., a set consisting of all nilpotent elements of \( R \);
- \( \text{Spec}(R) \) is a spectrum of ring \( R \), e.i., set of all prime ideals.

In this case \( \text{Nil}(R) = \mathfrak{M} \). Thus (1.33. Lemma) there exist such \( l \), that 
\[ (\text{Nil}(R))^l = \mathfrak{M}^l = 0. \]

Note that \( R \) here is a finite ring.

(iii) Let \( g_1(X) \equiv (1 + a_1X + a_2X^2 + \cdots + a_tX^t)^l. \) For any commutative ring holds 
\[ \alpha^l - \beta^l = (\alpha - \beta) \sum_{i=1}^{l} \alpha^{l-i} \beta^{i-1}. \]

If
- \( \alpha \) is given as \( 1 + a_1X + a_2X^2 + \cdots + a_tX^t \),
- \( \beta \) 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 coefficient of polynomial \( (\sum_{i=t+1}^{k} a_iX^i)^l \) are equal to 0, because \( a_{t+1}, a_{t+2}, \ldots, a_k \notin \mathfrak{M} \). 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) Let’s 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 \( |R[X]/(g_1(X))| = |R|^u < \infty \). Note that 
\[ R[X]/g_1(X) = \{ [r(X)] | h(X) \in R[X] \} \]
\[ \wedge \ h(X) = f(X)g_1(X) + r(X) \]
\[ \wedge \ \deg(r(X)) < \deg(g_1(X)) = u \]
(v) If $a = bc$, then $aR \subseteq bR$. Thus if $x \in aR$, then $x = ar$, where $r \in R$ and $x = ar = ber \in bR$.

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

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

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

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

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

Thus $(a_{11}, a_{12}, \ldots, a_{nn}) = \bar{a}_1 + \bar{a}_2 + \cdots + \bar{a}_n$. As $\varphi$ is an isomorphism, then $\varphi^{-1} : G^n \rightarrow R$ also is an isomorphism. Hence

$$\varphi^{-1}(a_{11}, a_{12}, \ldots, a_{nn}) = \varphi^{-1}(\bar{a}_1 + \bar{a}_2 + \cdots + \bar{a}_n)$$
$$= \varphi^{-1}(\bar{a}_1) + \varphi^{-1}(\bar{a}_2) + \cdots + \varphi^{-1}(\bar{a}_n).$$

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

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

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

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

is a homomorphism of rings.

$$\square \quad \phi(\sum_{i=0}^{m} (a_i + b_i) X^i) = \sum_{i=0}^{m} \phi(a_i + b_i) X^i = \sum_{i=0}^{m} (\phi(a_i) + \phi(b_i)) X^i$$
$$= \sum_{i=0}^{m} \phi(a_i) X^i + \sum_{i=0}^{m} \phi(b_i) X^i$$
$$= \phi(\sum_{i=0}^{m} a_i X^i) + \phi(\sum_{i=0}^{m} b_i X^i).$$
\[
\phi((\sum_{i=0}^{m} a_i X^i)(\sum_{j=0}^{n} b_j X^j)) = \phi\left(\sum_{k=0}^{m+n} \phi(\sum_{s=0}^{k} a_s b_{k-s}) X^k\right) \\
= \sum_{k=0}^{m+n} \phi(\sum_{s=0}^{k} a_s b_{k-s}) X^k \\
= \sum_{k=0}^{m+n} \sum_{x=0}^{k} \phi(a_x) \phi(b_{k-x}) X^k \\
= (\sum_{i=0}^{m} \phi(a_i) X^i)(\sum_{j=0}^{n} \phi(b_j) X^j) \\
= \phi(\sum_{i=0}^{m} a_i X^i)\phi(\sum_{j=0}^{n} b_j X^j). \quad \blacksquare
\]

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

\(\square\) (i) Let \(\sum_{i=0}^{m} a_i X^i \in S[X]\). As \(\phi : R \rightarrow S\) is an epimorphism, then
exist such \(a_1, a_2, \ldots, a_m \in R\), that \(\forall i \phi(a_i) = a_i\). Hence \(\phi(\sum_{i=0}^{m} a_i X^i) = \sum_{i=0}^{m} a_i X^i\).
(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). \(\blacksquare\)

2.16. Lemma. If \(\phi : R \rightarrow S\) is a ring isomorphism, then
\(R[X]/(\sum_{i=0}^{m} a_i X^i) \cong S[X]/(\sum_{i=0}^{m} \phi(a_i) X^i)\).

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

Let’s denote polynomials in consideration as: \(f = \sum_{i=0}^{m} a_i X^i\), \(\phi(f) = \sum_{i=0}^{m} \phi(a_i) X^i\),
\(p = \sum_{i=0}^{m} b_i X^i\), \(q = \sum_{i=0}^{m} c_i X^i\).
Hence mapping \( \phi : R \to S \) is an isomorphism, then \( p \equiv_R q \iff \phi(p) \equiv_S \phi(q) \).

Then
\[
p \equiv_R q, \\
p - q \equiv_R 0, \\
\exists r \in R[X] \ f_r = p - q, \\
\phi(r)\phi(f) = \phi(rf) = \phi(p - q) = \phi(p) - \phi(q), \\
\phi(p) - \phi(q) \equiv_S 0, \\
\phi(p) \equiv_S \phi(q).
\]

As mapping \( \phi : R \to S \) is an isomorphism, then \( p \equiv_R q \iff \phi(p) \equiv_S \phi(q) \).

Thus \( \tilde{\phi} \) is an isomorphism. 

\[ \boxdot \]

### 2.17. Lemma.

If \( \phi : R \to G_1 \times G_2 \times \cdots \times G_n \) is a ring homomorphism, then for all \( i \)
\[
\phi_i : R \to G_i : r \mapsto \text{pr}_i(\phi(r))
\]
is a ring homomorphism. Here \( \text{pr}_i(r_1, r_2, \ldots, r_n) = r_i \).

\[
\square \text{ Let } \phi(x) = (x_1, x_2, \ldots, x_n) \text{ and } \phi(y) = (y_1, y_2, \ldots, y_n), \text{ then}
\]
\[
\phi_i(x + y) = \text{pr}_i(\phi(x + y)) = \text{pr}_i(\phi(x) + \phi(y)) = x_i + y_i \\
\phi_i(x) + \phi_i(y) = \phi_i(x + y);
\]
\[
\phi_i(xy) = \text{pr}_i(\phi(xy)) = \text{pr}_i(\phi(x)\phi(y)) = x_i y_i \\
\phi_i(x)\phi_i(y). \quad \boxdot
\]

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

Here \( \phi_i(f) = \sum_{j=0}^m \text{pr}_j(\phi(a_j))X^j \).

\[
\square \text{ (i) Mapping } \phi_i : R \to G_i : r \mapsto \text{pr}_i(\phi(r)) \text{ is ring homomorphism (2.17. Lemma). As } \phi \text{ is an isomorphism, then } \phi_i \text{ is an epimorphism. Thus (2.15. Corollary)}
\]
\[
\phi_i : R[X] \to G_i[X] : p \mapsto \phi_i(p)
\]
is an epimorphism.
Assume that $\sum_{j=0}^n b_j X^j \equiv_R \sum_{j=0}^n c_j X^j$, i.e., they represent the same element from set $R[X]/(\sum_{j=0}^n a_j X^j)$. Let's denote polynomials in consideration as: $p \equiv \sum_{j=0}^n b_j X^j$, $q \equiv \sum_{j=0}^n c_j X^j$. Then

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

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

$$\begin{align*}
[p]_R &\equiv \{ g \mid g \equiv_R p \}, \\
[\phi_i(p)]_{G_i} &\equiv \{ h \mid h \equiv_{G_i} \phi_i(p) \}.
\end{align*}$$

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

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

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

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

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

Let's choose $p(X) \equiv \sum_{j=0}^k r_j X^j$. 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 $\Phi$ is not injective, might arise when $p \neq q$, but $\deg(p) = \deg(q)$. Let $q(X) = \sum_{j=0}^k r_j X^j$, $r_s \neq \rho_s$ and $\phi(\rho_s) = (b_1, b_2, \ldots, b_n)$. In expanded expression:

$$(a_{1s}, a_{2s}, \ldots, a_{ns}) = \phi(r_s) \neq \phi(\rho_s) = (b_1, b_2, \ldots, b_n).$$
Thus there exist such $\nu$, that $a_{\nu R} \neq b_\nu$.

$$\phi_\nu(p) = \sum_{j=0}^{k} \phi_\nu(r_j)X^j = \sum_{j=0}^{k} a_{\nu j}X^j = \sum_{j \neq \nu} a_{\nu j}X^j + a_{\nu \nu}X^\nu.$$ 

$$\phi_\nu(q) = \sum_{j=0}^{k} \phi_\nu(p_j)X^j = \sum_{j \neq \nu} \phi_\nu(p_j)X^j + \phi_\nu(p_\nu)X^\nu$$

$$= \sum_{j \neq \nu} \phi_\nu(p_j)X^j + b_\nu X^\nu.$$ 

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

(iii) Let

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

Thus $[p_1] \subseteq G_1[X]$ and $p_n \in G_n[X]$. As $\Phi$ 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 $[p_1]_{G_1} = [\phi_1(p)]_{G_1}$. From the definition of $\tilde{\phi}_i$, we have $\tilde{\phi}_i : [p]_R \rightarrow [\phi_i(p)]_{G_i}$ and

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

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

Let $\tilde{\phi}([p]_R) = \tilde{\phi}([0]_R)$, then $\forall i \tilde{\phi}_i([p]_R) = \tilde{\phi}_i([0]_R)$, 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 $\Phi : R[X] \rightarrow G_1[X] \times G_2[X] \times \cdots \times G_n[X]$ is bijective, then exists $p \in R[X]$, that $\Phi(p) = (r_1, r_2, \ldots, r_n)$. On the other hand $\Phi(p) = (\phi_1(p), \phi_2(p), \ldots, \phi_n(p))$. Thus $r_i = \phi_i(p)$, therefore $\phi_i(p) = r_i \phi_i(f) = \phi_i(p) \phi_i(f) = \phi_i(pf)$. Hence

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

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

From all the above we conclude:

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

is an isomorphism. $lacksquare$

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 $\mathbb{Z}_m \cong \mathbb{Z}_m$, then there exist such $n$, that $g(X)$ divides $X^n - 1$. 

27
(i) Let \( \alpha = a_1^\ast a_2^\ast \ldots a_k^\ast, \beta = b_1^\ast b_2^\ast \ldots b_k^\ast \), where \( a, b \in \mathbb{Z}_m \), then \( \alpha + \beta = (a + b)^{\ast} \). Let denote by \( \mathbb{Z}_m(a_1, a_2, \ldots, a_k) \) the smallest extension of ring \( \mathbb{Z}_m \), containing all elements \( a_1, a_2, \ldots, a_k \). Thus \( \mathbb{Z}_m(a_1, a_2, \ldots, a_k) \) consists of sums:

\[
\sum_{x \in \mathbb{Z}_m} a_x a_1^\ast a_2^\ast \ldots a_k^\ast,
\]

where \( a_x \in \mathbb{Z}_m \) and \( \bar{x} = (x_1, x_2, \ldots, x_k) \). There all \( \bar{x} \) are distinct.

(ii) As \( \mathbb{Z}_m(a_1, a_2, \ldots, a_k) \) is an integral extension, then for each \( a_i \) there exists such monic polynomial

\[
p_i(X) = X^{m_i} + b_1m_{i-1}X^{m_i-1} + \ldots + b_1X + b_0,
\]

that \( p_i(a_i) = 0 \). Hence

\[
a_i^{m_i} = -b_1m_{i-1}a_i^{m_i-1} - \ldots - b_1a_i - b_0.
\]

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

\[
\sum_{x \in \mathbb{Z}_m} a_x a_1^\ast a_2^\ast \ldots a_k^\ast,
\]

where all \( \bar{x} = (x_1, x_2, \ldots, x_k) \) are distinct and all \( x_i < m_i \). Then count of such sums is finite, because ring \( \mathbb{Z}_m \) is finite. Thus ring \( \mathbb{Z}_m(a_1, a_2, \ldots, a_k) \) is finite.

(iii) As \( S \simeq \mathbb{Z}_m(a_1, a_2, \ldots, a_k) \) is a finite ring, then (1.45. Theorem)

\[
S \simeq S_1 \times S_2 \times \ldots \times S_t,
\]

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

\[
S[X]/(g) \simeq S_1[X]/(\phi_1(g)) \times S_2[X]/(\phi_2(g)) \times \ldots \times S_t[X]/(\phi_t(g)).
\]

Here

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

is an isomorphism, where

\[
\phi : S \to S_1 \times S_2 \times \ldots \times S_t
\]

is an isomorphism, \( \phi_1(g) = \sum_{j=0}^k p_j(\phi(a_j))X^j \) and \( a_0 = 1 \). Thus

\[
\phi_i(g) = 1s_i + \sum_{j=1}^k p_j(\phi(a_j))X^j.
\]

(2.13. Lemma) \( S[X]/(\phi_1(g)) \) is a finite set, thus \( S[X]/(g) \) is a finite ring. Therefore all classes \([1], [X], [X^2], [X^3], \ldots, [X^n], \ldots \) can’t be distinct. Thus there exist such \( n \geq 0 \) and \( \nu > 0 \), that \( [X^n] = [X^{n+\nu}] \) or \( [X^n(X^n - 1)] = [0] \). Thus thee exist such \( q : X \to S[X] \), that \( q(X)q(X) = X^n(X^n - 1) \). As \( q(0) = 1 \), then \( q(X) = X^\nu r(X) \). Hence \( X^\nu q(X)r(X) = X^\nu(X^n - 1) \). It is possible only if \( g(X)r(X) = X^n - 1 \).
2.20. Proposition. If integral extension \( f \) of \( \mathbb{Z}_m \cong \mathbb{Z}_m \) is a rational series, then \( f \) is semiperiodic.

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

\[
f = \frac{h}{g} = \frac{h(X^n - 1)}{g(X^n - 1)} = \frac{a_0^{-1} h}{X^n - 1} \cdot \frac{X^n - 1}{a_0^{-1} g} = \frac{a_0^{-1} h}{a_0^{-1} g} \cdot \frac{1}{X^n - 1} = -a_0^{-1} hr \sum_{k=0}^{\infty} X^{kn}
\]

Assume that \( -a_0^{-1} hr = \sum_{\nu=0}^{\sigma} b_{\nu} X^\nu \), then \( f = \sum_{\nu=0}^{\sigma} b_{\nu} X^\nu \sum_{k=0}^{\infty} X^{kn} \).

If \( n = 1 \), then

\[
f = \sum_{\nu=0}^{\sigma} b_{\nu} X^\nu \sum_{k=0}^{\infty} X^k = (b_0 + b_1 X + b_2 X^2 + \ldots + b_{\sigma} X^\sigma) (1 + X + X^2 + \ldots + X^n + \ldots)
\]

If \( \sigma < n \), then

\[
f = \sum_{\nu=0}^{\sigma} b_{\nu} X^\nu \sum_{k=0}^{\infty} X^{kn} = (b_0 + b_1 X + b_2 X^2 + \ldots + b_{\sigma} X^\sigma) (1 + X^n + X^{2n} + \ldots + X^{kn} + \ldots)
\]

If \( \sigma = n + \tau \) un 0 \( \leq \tau < n \), then

\[
f = \sum_{\nu=0}^{\sigma} b_{\nu} X^\nu \sum_{k=0}^{\infty} X^{kn} = (b_0 + b_1 X + b_2 X^2 + \ldots + b_{\sigma} X^\sigma)(1 + X^n + X^{2n} + \ldots + X^{kn} + \ldots)
\]

28
\[ f = \sum_{k=0}^{n-1} b_k X^k + \sum_{k=1}^{\infty} \left( \sum_{i=0}^{r} (b_i + b_{n+i}) X^{kn+i} + \sum_{i=\tau+1}^{n-1} b_i X^{kn+i} \right) \]

If \( \sigma = mn + \tau \) un \( 0 \leq \tau < n \), then

\[ f = \sum_{a=0}^{\sigma} b_a X^a \sum_{k=0}^{\infty} X^{kn} \]

\[ = (b_0 + b_1 X + b_2 X^2 + \ldots + b_{n-1} X^{n-1} + b_n X^n + \ldots + b_{mn+\tau} X^{mn+\tau}) \times (1 + X^n + X^{2n} + \ldots + X^{kn} + \ldots) \]

\[ = b_0 + b_1 X + b_2 X^2 + \ldots + b_{n-1} X^{n-1} + (b_0 + b_n) X^n + (b_1 + b_{n+1}) X^{n+1} + \ldots + (b_0 + b_n + b_{n+1} + \ldots + b_{(m-1)n+1}) X^{(m-1)n} + \ldots \]

\[ + (b_1 + b_{n+1} + b_{2n+1} + \ldots + b_{(m-1)n+1}) X^{(m-1)n+1} + \ldots \]

\[ + (b_0 + b_n + \ldots + b_{mn}) X^{mn} + (b_1 + b_{n+1} + \ldots + b_{mn+1}) X^{mn+1} + \ldots \]

\[ + (b_0 + b_n + \ldots + b_{mn} + b_{mn+1} + \ldots + b_{mn+\tau}) X^{mn+\tau} \]

\[ + (b_{r+1} + b_{n+\tau+1} + \ldots + b_{(m-1)n+\tau+1}) X^{mn+\tau+1} + \ldots \]

\[ = \sum_{k=0}^{m-1} \sum_{i=0}^{n-1} \left( \sum_{j=0}^{k} b_{i+jn} \right) X^{nk+i} \]

\[ + \sum_{k=m}^{\infty} \left( \sum_{i=0}^{m} \left( \sum_{j=0}^{k} b_{i+jn} \right) X^{kn+i} + \sum_{i=\tau+1}^{n-1} \left( \sum_{j=0}^{m-1} b_{i+jn} \right) X^{kn+i} \right) \]

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

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

2.22. Example. \( f(X) = \frac{X^2 + 2X - 1}{X^2 + X + 1} \), where polynomials are elements of ring \( \mathbb{Z}_4[X] \).

\[ f(X) = \frac{X^2 + 2X - 1}{X^2 + X + 1} = \frac{(X^2 + 2X - 1)(X^3 - 1)}{(X^2 + X + 1)(X^3 - 1)} \]

\[ = \frac{(X^2 + 2X - 1)(X - 1)}{X^3 - 1} \]

\[ = -(1 - 3X + X^2 + X^3)(1 + X^3 + X^6 + X^9 + \ldots) \]

Let’s consider the general expression: \( \sigma = n = 3 \) and \( \tau = 0 \).

\[ f(X) = (b_0 + b_1 X + b_2 X^2 + b_3 X^3)(1 + X^3 + X^6 + X^9 + \ldots) \]

\[ = b_0 + b_1 X + b_2 X^2 + \sum_{k=1}^{\infty} ((b_0 + b_3) X^{3k} + b_1 X^{3k+1} + b_2 X^{3k+2}) \]
In our case:

\[ f(X) = -1 + 3X - X^2 + \sum_{k=1}^{\infty} ((-1 - 1)X^{3k} + 3X^{3k+1} - X^{3k+2}) \]

\[ = -1 + 3X - X^2 + \sum_{k=1}^{\infty} (-2X^{3k} + 3X^{3k+1} - X^{3k+2}) \]

3. Mealy machines

We will consider mappings 

\[ \mu[f] : g(X) \mapsto f(X)g(X), \]

\[ \alpha[f] : g(X) \mapsto f(X) + g(X), \]

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 \( f(X) = \sum_{k=0}^{\infty} a_kX^k \).

3.3. Corollary.

- \( f = a_0 + \sigma(f)X \);
- \( (1 - aX)^{-1} = \sum_{k=0}^{\infty} a^kX^k \);
- if \( f = \frac{1}{1 - aX} \) 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 \( \omega \)-determined function. Function \( \zeta \) defines set

\[ Q_{\zeta} = \{ \zeta_u \mid u \in A^* \} \]

where \( \zeta_u \) is restriction of function \( \zeta \). If set \( Q_f \) is finite, then \( \zeta \) is called a finitely determined function.

3.5. Theorem. If \( f = \frac{1}{1 - X} \), then \( \mu[f] \) is finitely determined function, whose restriction set \( Q_f = \{ \mu[f] \circ \alpha[s] \mid s \in R \} \).
Let \( f = \frac{1}{1-X} \). Define \( M_f = \langle Q_f, R, \circ, \ast \rangle \):

- with set \( Q_f = \{ \alpha[s]\mu[f] \mid s \in R \} \) of states and
- alphabet \( R \),
- \( Q \times R \overset{\circ}{\longrightarrow} Q : \alpha[s]\mu[f] \circ r = \alpha[s+r]\mu[f] \),
- \( Q \times A \overset{\ast}{\longrightarrow} A : \alpha[s]\mu[f] \ast r = s + r \).

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

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

and \( \Gamma(M_2) = (q, p) = (\alpha[0]\mu[f], \alpha[1]\mu[f]) \).

\[
\begin{array}{c|c|c}
M_2 & 0/0 & 1/0 \\
\hline
0/1 & p & q \\
1/1 & q & p
\end{array}
\]

\[
\begin{array}{c|c|c}
M_2^{-1} & 0/0 & 1/0 \\
\hline
0/1 & p^{-1} & q^{-1} \\
1/1 & q^{-1} & p^{-1}
\end{array}
\]

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

\[
g[\alpha]\mu[f] = (r + s_0 + \sum_{k=1}^{\infty} s_kX^k)\mu[f] = (r + s_0) f(X) + f(X) \sum_{k=1}^{\infty} s_kX^k
\]

\[
= (r + s_0) + (r + s_0)X + (r + s_0)X^2
+ (1 + X + X^2)(s_1X + s_2X^2 + s_3X^3 + s_4X^4 + \cdots )
= (r + s_0) + (r + s_0)X + (r + s_0)X^2
+ s_1X + (s_1 + s_2)X^2
+ (s_1 + s_2 + s_3)X^3 + (s_2 + s_3 + s_4)X^4 + (s_3 + s_4 + s_5)X^5 + \cdots
\]

\[
= (r + s_0) + (r + s_0 + s_1)X + (r + s_0 + s_1 + s_2)X^2
+ (s_1 + s_2 + s_3)X^3 + (s_2 + s_3 + s_4)X^4 + (s_3 + s_4 + s_5)X^5 + \cdots
\]

31
\[ g\mu[f] = s_0 + (s_0 + s_1)X + (s_0 + s_1 + s_2)X^2 + (s_1 + s_2 + s_3)X^3 + \cdots \]
\[ = s_0 + (s_0 + s_1)X + \sum_{k=0}^{\infty} (s_k + s_{k+1} + s_{k+2})X^{k+2}. \]

Hence

\[ g\mu_0[f] = r + s_0 + (r + s_0 + s_1)X + (s_0 + s_1 + s_2)X^2 + (s_1 + s_2 + s_3)X^3 + \cdots \]
\[ = r + s_0 + (r + s_0 + s_1)X + \sum_{k=0}^{\infty} (s_k + s_{k+1} + s_{k+2})X^{k+2}, \]

\[ g\mu_1[f] = 2r + s_0 + (r + s_0 + s_1)X + (s_0 + s_1 + s_2)X^2 + (s_1 + s_2 + s_3)X^3 + \cdots \]
\[ = 2r + s_0 + (r + s_0 + s_1)X + \sum_{k=0}^{\infty} (s_k + s_{k+1} + s_{k+2})X^{k+2}, \]

\[ g\mu_2[f] = 2r + s_0 + (r + s_0 + s_1)X + (s_0 + s_1 + s_2)X^2 + (s_1 + s_2 + s_3)X^3 + \cdots \]
\[ = 2r + s_0 + (r + s_0 + s_1)X + \sum_{k=0}^{\infty} (s_k + s_{k+1} + s_{k+2})X^{k+2}, \]

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

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

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

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

Let’s introduce notation \( \mu u = \mu_u[f] \) for each \( u \in R^* \).

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

From the above, it follows that:

\[
\begin{align*}
\mu & = \mu 0 = \mu u00 \quad \rightarrow \quad s_0 + (s_0 + s_1)X \\
\mu 1 & = \mu 01 = \mu u01 \quad \rightarrow \quad 1 + s_0 + (1 + s_0 + s_1)X \\
\mu 10 & = \mu u10 \quad \rightarrow \quad 1 + s_0 + (s_0 + s_1)X \\
\mu 11 & = \mu u11 \quad \rightarrow \quad s_0 + (1 + s_0 + s_1)X
\end{align*}
\]

What happens if \( R = GF(4) \)?
2. Figure: Machine defined by $1 + X + X^2$ in field $GF(2)$.

\[
\begin{array}{|c|c|c|c|}
\hline
x \backslash y & 0 & 1 & a \\
\hline
0 & 0 & 1 & a \\
1 & 0 & 1 & a \\
\hline
\end{array}
\begin{array}{|c|c|c|c|}
\hline
\text{addition } x + y & 0 & 1 & a \\
\hline
0 & 0 & 1 & a \\
1 & 0 & 1 & a \\
\hline
\end{array}
\begin{array}{|c|c|c|c|}
\hline
\text{multiplication } xy & 0 & 1 & a \\
\hline
0 & 0 & 1 & a \\
1 & 0 & 1 & a \\
\hline
\end{array}
\]

\[
\begin{align*}
\mu &= \mu_0 = \mu u00 \\
\mu1 &= \mu01 = \mu u01 \\
\mu a &= \mu0a = \mu u0a \\
\mu b &= \mu0b = \mu u0b \\
\mu 10 &= \mu u10 \\
\mu 11 &= \mu u11 \\
\mu 1a &= \mu u1a \\
\mu 1b &= \mu u1b \\
\mu a0 &= \mu ua0 \\
\mu a1 &= \mu ua1 \\
\mu aa &= \mu uaa \\
\mu ab &= \mu uab \\
\mu b0 &= \mu ub0 \\
\mu b1 &= \mu ub1 \\
\mu ba &= \mu uba \\
\mu bb &= \mu ubb \\
\end{align*}
\]

\[
\begin{align*}
&\rightarrow s_0 + (s_0 + s_1)X \\
&\rightarrow 1 + s_0 + (1 + s_0 + s_1)X \\
&\rightarrow a + s_0 + (a + s_0 + s_1)X \\
&\rightarrow b + s_0 + (b + s_0 + s_1)X \\
&\rightarrow 1 + s_0 + (s_0 + s_1)X \\
&\rightarrow s_0 + (1 + s_0 + s_1)X \\
&\rightarrow b + s_0 + (a + s_0 + s_1)X \\
&\rightarrow a + s_0 + (b + s_0 + s_1)X \\
&\rightarrow a + s_0 + (s_0 + s_1)X \\
&\rightarrow b + s_0 + (1 + s_0 + s_1)X \\
&\rightarrow s_0 + (a + s_0 + s_1)X \\
&\rightarrow 1 + s_0 + (b + s_0 + s_1)X \\
&\rightarrow b + s_0 + (s_0 + s_1)X \\
&\rightarrow a + s_0 + (1 + s_0 + s_1)X \\
&\rightarrow 1 + s_0 + (a + s_0 + s_1)X \\
&\rightarrow s_0 + (b + s_0 + s_1)X
\end{align*}
\]
<table>
<thead>
<tr>
<th></th>
<th>$\mu$</th>
<th>$\mu_1$</th>
<th>$\mu a$</th>
<th>$\mu b$</th>
<th>$\mu_{10}$</th>
<th>$\mu_{11}$</th>
<th>$\mu_{1a}$</th>
<th>$\mu_{1b}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\mu$</td>
<td>$\mu_{10}$</td>
<td>$\mu a_0$</td>
<td>$\mu b_0$</td>
<td>$\mu$</td>
<td>$\mu_{10}$</td>
<td>$\mu a_0$</td>
<td>$\mu b_0$</td>
</tr>
<tr>
<td>1</td>
<td>$\mu_1$</td>
<td>$\mu_{11}$</td>
<td>$\mu a_1$</td>
<td>$\mu b_1$</td>
<td>$\mu_1$</td>
<td>$\mu_{11}$</td>
<td>$\mu a_1$</td>
<td>$\mu b_1$</td>
</tr>
<tr>
<td>a</td>
<td>$\mu a$</td>
<td>$\mu a a_1$</td>
<td>$\mu a b_1$</td>
<td>$\mu a b_1$</td>
<td>$\mu a$</td>
<td>$\mu a a_1$</td>
<td>$\mu a b_1$</td>
<td>$\mu a b_1$</td>
</tr>
<tr>
<td>b</td>
<td>$\mu b$</td>
<td>$\mu b a_1$</td>
<td>$\mu b b_1$</td>
<td>$\mu b b_1$</td>
<td>$\mu b$</td>
<td>$\mu b a_1$</td>
<td>$\mu b b_1$</td>
<td>$\mu b b_1$</td>
</tr>
<tr>
<td>*</td>
<td>$\mu$</td>
<td>$\mu_1$</td>
<td>$\mu a$</td>
<td>$\mu b$</td>
<td>$\mu_{10}$</td>
<td>$\mu_{11}$</td>
<td>$\mu_{1a}$</td>
<td>$\mu_{1b}$</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>a</td>
<td>b</td>
<td>1</td>
<td>0</td>
<td>b</td>
<td>a</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>b</td>
<td>a</td>
<td>0</td>
<td>1</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>0</td>
<td>1</td>
<td>b</td>
<td>a</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td>1</td>
<td>0</td>
<td>a</td>
<td>b</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$\mu a_0$</th>
<th>$\mu a_1$</th>
<th>$\mu a a_1$</th>
<th>$\mu a b_1$</th>
<th>$\mu b_0$</th>
<th>$\mu b_1$</th>
<th>$\mu b a_1$</th>
<th>$\mu b b_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\mu$</td>
<td>$\mu_{10}$</td>
<td>$\mu a_0$</td>
<td>$\mu b_0$</td>
<td>$\mu$</td>
<td>$\mu_{10}$</td>
<td>$\mu a_0$</td>
<td>$\mu b_0$</td>
</tr>
<tr>
<td>1</td>
<td>$\mu_1$</td>
<td>$\mu_{11}$</td>
<td>$\mu a_1$</td>
<td>$\mu b_1$</td>
<td>$\mu_1$</td>
<td>$\mu_{11}$</td>
<td>$\mu a_1$</td>
<td>$\mu b_1$</td>
</tr>
<tr>
<td>a</td>
<td>$\mu a$</td>
<td>$\mu a a_1$</td>
<td>$\mu a b_1$</td>
<td>$\mu a b_1$</td>
<td>$\mu a$</td>
<td>$\mu a a_1$</td>
<td>$\mu a b_1$</td>
<td>$\mu a b_1$</td>
</tr>
<tr>
<td>b</td>
<td>$\mu b$</td>
<td>$\mu b a_1$</td>
<td>$\mu b b_1$</td>
<td>$\mu b b_1$</td>
<td>$\mu b$</td>
<td>$\mu b a_1$</td>
<td>$\mu b b_1$</td>
<td>$\mu b b_1$</td>
</tr>
<tr>
<td>*</td>
<td>$\mu a_0$</td>
<td>$\mu a_1$</td>
<td>$\mu a a_1$</td>
<td>$\mu a b_1$</td>
<td>$\mu b_0$</td>
<td>$\mu b_1$</td>
<td>$\mu b a_1$</td>
<td>$\mu b b_1$</td>
</tr>
<tr>
<td>0</td>
<td>a</td>
<td>b</td>
<td>0</td>
<td>1</td>
<td>b</td>
<td>a</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>b</td>
<td>a</td>
<td>1</td>
<td>0</td>
<td>a</td>
<td>b</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>a</td>
<td>0</td>
<td>1</td>
<td>a</td>
<td>b</td>
<td>1</td>
<td>0</td>
<td>b</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>0</td>
<td>b</td>
<td>a</td>
<td>0</td>
<td>1</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>
References


