9. Finite fields.

A. Ushakov

MA503, March 30, 2022

Contents

The first half of today's lecture is similar to lecture #1, where we discussed the fundamental theorem of arithmetic and congruence relation mod n. Here we do the same for polynomials. The second half of the lecture is devoted to field extensions and their properties.

- Unique factorization in $F[x]$.
- Ideal.
- Ideals in $F[x]$.
- Quotient ring.
- Kronecker's theorem.
- Multiplicative group of a field.
- Vector space. Subspace. Basis. Dimension.
- Extension field as a vector space.
- Adjoining elements.
- Splitting field.

Unique factorization in $F[x]$

Lemma

Suppose that $f(x)$ is irreducible. Then for any $g(x), h(x)$

$$f(x) \mid g(x)h(x) \quad \Rightarrow \quad f(x) \mid g(x) \quad \textit{or} \quad f(x) \mid h(x)$$

If $f(x) \mid g(x)$, then there is nothing to prove. So, suppose that $f(x) \nmid g(x)$. Then

$$\begin{aligned}
f(x) \nmid g(x) \quad &\Rightarrow \quad \gcd(f(x), g(x)) = 1 && (f(x) \text{ is irreducible and } f(x) \nmid g(x)) \\
&\Rightarrow \quad 1 = \alpha(x)f(x) + \beta(x)g(x) && (\text{Bezout identity}) \\
&\Rightarrow \quad h(x) = \alpha(x)h(x)f(x) + \beta(x)g(x)h(x) && (\text{multiplied by } h(x)) \\
&\Rightarrow \quad f(x) \mid h(x).
\end{aligned}$$

Theorem

Every non-constant $f(x) \in F[x]$ can be expressed as

$$f(x) = c \cdot f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_k(x),$$

where $c \in F$ and $f_1(x), \ldots, f_k(x)$ are monic and irreducible. This expression is unique up to a permutation of factors

Congruences modulo $f(x)$

Let F be a field and $f(x) \in F[x]$.

Definition

$g(x), h(x) \in F[x]$ are **congruent modulo $f(x)$** and write

$$g(x) \equiv_{f(x)} h(x) \quad \text{or} \quad g(x) \equiv h(x) \mod f(x)$$

if they give the same remainder when divided by $f(x)$.

- $x^2 + 1 \equiv 0 \mod x^2 + 1$ in $\mathbb{Z}_2[x]$.
- $x^3 + x \equiv 0 \mod x^2 + 1$ in $\mathbb{Z}_2[x]$.
- $x^3 + 1 \equiv x + 1 \mod x^2 + 1$ in $\mathbb{Z}_2[x]$.
- $4x^3 + 3x^2 \equiv x^3 + x^2 + 4x + 3 \mod 3x^2 + 4x + 2$ in $\mathbb{Z}_5[x]$.

Theorem

$\equiv_{f(x)}$ is an equivalence relation on $F[x]$.

Therefore, equivalence classes (**congruence classes modulo $f(x)$**) of polynomials

$$[g(x)] = \{h(x) \mid h(x) \equiv_{f(x)} g(x)\}$$

define a partition of $F[x]$. Denote the set of all equivalence classes by $F[x]/f(x)$.

Theorem

$g(x) \equiv_{f(x)} h(x) \quad \Leftrightarrow \quad f(x) \mid (g(x) - h(x)).$

"$\Rightarrow$"

$$\begin{aligned} g(x) \equiv_{f(x)} h(x) \quad &\Leftrightarrow \quad \begin{cases} g(x) = \alpha(x)f(x) + r(x) \\ h(x) = \beta(x)f(x) + r(x) \end{cases} \\ &\Rightarrow \quad g(x) - h(x) = (\alpha(x) - \beta(x))f(x) \\ &\Rightarrow \quad f(x) \mid (g(x) - h(x)). \end{aligned}$$

"$\Leftarrow$" (Contrapositive)

$$\begin{aligned} g(x) \not\equiv_{f(x)} h(x) \quad &\Leftrightarrow \quad \begin{cases} g(x) = \alpha(x)f(x) + r_1(x) \\ h(x) = \beta(x)f(x) + r_2(x) \end{cases} \\ &\Rightarrow \quad g(x) - h(x) = (\alpha(x) - \beta(x))f(x) + (r_1(x) - r_2(x)), \\ &\quad\ \text{where } r_1(x) - r_2(x) \neq 0 \\ &\Rightarrow \quad f(x) \nmid (g(x) - h(x)). \end{aligned}$$

Arithmetic of congruences

Fix the modulus $f(x) \neq 0$. For $g(x), h(x) \in F[x]$ define

- $[\mathrm{g(x)}] + [\mathrm{h(x)}] = [g(x) + h(x)]$ – *the sum of congruences,*
- $[\mathrm{g(x)}] \cdot [\mathrm{h(x)}] = [g(x) \cdot h(x)]$ – *the product of congruences.*

Proposition

The defined above operations $+$ and $\cdot$ are well defined on $F[x]/f(x)$, i.e., do not depend on a choice of representatives.

Suppose that $[g_1] = [g_2]$ and $[h_1] = [h_2]$. By definition,

$$\begin{matrix} [g_1] = [g_2] \\ [h_1] = [h_2] \end{matrix} \quad \Leftrightarrow \quad \begin{matrix} f \mid g_2 - g_1 \\ f \mid h_2 - h_1 \end{matrix} \quad \Leftrightarrow \quad \begin{matrix} g_2 - g_1 = \alpha f \\ h_2 - h_1 = \beta f \end{matrix}$$

But then

$$(g_2 + h_2) - (g_1 + h_1) = \alpha f + \beta f = (\alpha + \beta) f,$$

which means that $[g_1 + h_1] = [g_2 + h_2]$. Similarly,

$$g_2 h_2 - g_1 h_1 = g_2(h_2 - h_1) - h_1(g_2 - g_1) = g_2 \beta f - h_1 \alpha f = (g_2 \beta - h_1 \alpha) f,$$

which means that $[g_2 h_2] = [g_1 h_1]$.

$F[x]/f(x)$ is a ring

Notice that $+$ and $\cdot$ on $F[x]/f(x)$ satisfies the following properties:

- $+$ is associative and commutative.
- $[0]$ is the additive identity.
- $[-g(x)]$ is the additive inverse of $[g(x)]$.
- $\cdot$ is associative and commutative.
- $[1]$ is the multiplicative identity.
- $(g_1(x) + g_1(x))h(x) = g_1(x)h(x) + g_1(x)h(x)$.
- $h(x)(g_1(x) + g_1(x)) = h(x)g_1(x) + h(x)g_1(x)$.

Therefore, the following theorem holds.

Theorem

$(F[x]/f(x), +, \cdot)$ is a ring, called a ***quotient ring*** *of $F[x]$.*

(R1) $(F[x]/f(x), +)$ is an abelian group with the identity I.

(R2) Multiplication is associative and $[1]$ is the unity.

(R3) Distributive law.

$F[x]/f(x)$: normal forms and operations

Suppose that $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}_p[x]$.

Theorem (Unique representatives modulo $f(x)$)

For every $g(x) \in \mathbb{Z}_p[x]$ there exists a unique polynomial $r(x) \in \mathbb{Z}_p[x]$ satisfying

(a) $\deg(r(x)) < \deg(f(x))$,

(b) $[g(x)] = [r(x)]$.

(Existence) Divide $g(x)$ by $f(x)$: $g(x) = q(x)f(x) + r(x)$. Both conditions hold for the remainder of division $r(x)$.

(Uniqueness) Suppose that both conditions hold for $h_1(x), h_2(x)$. Then

$$\begin{aligned} [r_1(x)] = [r_2(x)] \quad &\Rightarrow \quad f(x) \mid r_2(x) - r_1(x) \\ &\Rightarrow \quad r_2(x) - r_1(x) = 0 \text{ (because } \deg(r_2(x) - r_1(x)) < \deg(f(x))\text{)}. \end{aligned}$$

$E = \mathbb{Z}_p[x]/f(x)$ can be viewed as a set of polynomials of degree less $\deg(f(x))$.
In particular, $|E| = p^n$. Addition and multiplication in E is done modulo $f(x)$.

Example: $\mathbb{Z}_2[x]/x^3+x+1$

$\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ contains 8 elements $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.

The multiplication table for $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ is defined as follows:

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

The addition table for $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ is defined as follows:

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Given the multiplication table it is very easy to find multiplicative inverses, e.g.

$$1^{-1}=1 \qquad x^{-1}=x^2+1 \qquad (x+1)^{-1}=x^2+x \qquad (x^2)^{-1}=x^2+x+1.$$

Kronecker's theorem

For a field F the Kronecker's theorem allows to construct an extension of F.

Proposition

If $f(x) \in F[x]$ is non-constant and irreducible, then $E = F[x]/\langle f(x)\rangle$ is a field.

$$\begin{aligned}
[g(x)] \in E \text{ is non-trivial} \quad &\Rightarrow \quad [g(x)] \neq [0] \quad \Rightarrow \quad f(x) \nmid g(x) \\
&\Rightarrow \quad 1 = \gcd(f(x), g(x)) \\
&\Rightarrow \quad 1 = \alpha(x)f(x) + \beta(x)g(x) \quad \text{for some } \alpha(x), \beta(x) \\
&\Rightarrow \quad [1] = [\alpha(x)] \cdot [f(x)] + [\beta(x)] \cdot [g(x)] \\
&\Rightarrow \quad [1] = [\alpha(x)] \cdot [0] + [\beta(x)] \cdot [g(x)] \\
&\Rightarrow \quad [1] = [\beta(x)] \cdot [g(x)]. \\
&\Rightarrow \quad [g(x)] \text{ is a unit.}
\end{aligned}$$

$f(x) \in \mathbb{Z}_p[x]$ is irreducible and $\deg(f) = n \quad \Rightarrow \quad \mathbb{Z}_p[x]/f(x)$ is a field of size p^n.

Definition

A finite field of size p^n is called the **Galois field** and is denoted $\mathrm{GF}(p^n)$.

Theorem

For every prime p and $n \in \mathbb{N}$ there is an irreducible polynomial $f(x)$ of degree n.

No proof.

Finite field: classification

Theorem

- *Every finite field F has size p^n for some prime p and $n \in \mathbb{N}$.*
- *For every prime power p^n there exists a field F of size p^n.*
- *Two fields of size p^n are isomorphic.*

Thus, every finite field $\mathrm{GF}(p^n)$ can be implemented as a set of polynomials with coefficients from $\mathbb{Z}_p$ modulo an irreducible polynomial of degree n, i.e., using the Kronecker's theorem.

Theorem (A corollary of the Kronecker's theorem)

For any non-constant irreducible polynomial $f(x) \in F[x]$ there is an extension field E of F and $\alpha \in E$ such that $f(\alpha) = 0$.

We claim that $E = F[z]/f(z)$ is a required field.

- E contains F (as a subfield of constant polynomials);
- $[z]$ is a zero of f, because $f([z]) = [f(z)] = [0]$.

Multiplicative group of a field

Definition

Let $(F, +, \cdot)$ be a field. The set $F^* = \{a \in F \mid a \neq 0\}$ is a group under multiplication $\cdot$, called the **multiplicative group** of a field.

For instance, $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid a \neq 0\} = U_p$.

Theorem

Any finite subgroup G of F^* is cyclic. In particular, the multiplicative group of a finite field is cyclic.

- G is finite abelian $\Rightarrow$ $G \simeq \mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$.
- Let $m = \mathrm{lcm}(p_1^{r_1}, \ldots, p_n^{r_n})$. Every element in G is a zero of $x^m - 1 \in F[x]$.
- $m \geq p_1^{r_1} \ldots p_n^{r_n}$ because a polynomial of degree m can not have more than m distinct zeros in a field F.
- Hence, $m = \mathrm{lcm}(p_1^{r_1}, \ldots, p_n^{r_n}) = p_1^{r_1} \ldots p_n^{r_n}$

Thus, G has an element of order $p_1^{r_1} \ldots p_n^{r_n}$ and is cyclic.

Corollary

There exists a primitive root mod p for every prime p.

Because $U_p = \mathbb{Z}_p^*$.

Primitive roots in $\mathrm{GF}(p^n)$

Definition

$\alpha \in \mathrm{GF}(p^n)$ such that $\langle \alpha \rangle = \mathrm{GF}(p^n)^*$ is called a **primitive root**.

$\alpha \in \mathrm{GF}(p^n)$ is a primitive root $\quad \Leftrightarrow \quad |\alpha| = p^n - 1$.

Since $|\,\mathrm{GF}(2^3)^*| = 7$ *is prime, every* $\alpha \neq 0, 1$ *is a primitive root in* $\mathrm{GF}(8)$.

Since $|\,\mathrm{GF}(2^4)^*| = 15 = 3 \cdot 5$ *is not prime. The order of every element* $\alpha \in \mathrm{GF}(8)$ *divides* 15*, i.e.,* $|\alpha| = 1, 3, 5, 15$ *and to check that* α *is a primitive root it is sufficient to check that* $|\alpha| \neq 3, 5$.

$x^4 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible and $\mathrm{GF}(16) \simeq \mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$. To check if x is a primitive root we check that

$$x^3 \neq 1 \text{ modulo } x^4 + x + 1 \quad \text{and} \quad x^5 = x^2 + x \neq 1 \text{ modulo } x^4 + x + 1.$$

Since $|\,\mathrm{GF}(2^5)^*| = 31$ *is prime, every* $\alpha \neq 0, 1$ *is a primitive root in* $\mathrm{GF}(32)$.

Proposition

If $\mathrm{PPF}(p^n - 1) = p_1^{a_1} \dots p_k^{a_k}$*, then* $\alpha \in \mathrm{GF}(p^n)^*$ *is a primitive root* $\quad \Leftrightarrow \quad \alpha^{\frac{p^n - 1}{p_i}} \neq 1$.

Rabin's test of irreducibility (can be skipped)

Proposition

If E is a splitting field over F and $f(x) \in F[x]$ an irreducible polynomial that has a zero in E, then $f(x)$ has all zeros in E.

Consider a polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree $n = p_1^{a_1} \dots p_k^{a_k}$. Let $n_i = \frac{n}{p_i}$.

If $f(x)$ is irreducible, then $f(x)$ divides $x^{p^n} - x$ and $\gcd(f(x), x^{p^{n_i}} - x) = 1$.

If $f(x) = f_1(x) \dots f_m(x)$ where $\deg(f_i) \nmid \deg(f)$, then $f(x)$ does not divide $x^{p^n} - x$.

If $f(x) = f_1(x) \dots f_m(x)$ where $\forall i \ \deg(f_i) \mid \deg(f)$, then $\gcd(f(x), x^{p^{n_i}} - x) \neq 1$.

Theorem

Then $f(x)$ is irreducible if and only if

- $\gcd(f(x), x^{p^{n_i}} - x) = 1$ *for each* $i = 1, \dots, k$
- $f(x)$ *divides* $x^{p^n} - x$.

Multiplicative group of the field $\mathbb{Z}_2[x]/x^3 + x + 1$

$E = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ has 8 elements $\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$.

The multiplication table for $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ is defined as follows:

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Its multiplicative group has 7 elements

$$E^* = \{1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$$

and, hence, is isomorphic to $\mathbb{Z}_7$. Every nontrivial (not 1) element of E^* is primitive. E.g., $x + 1$ is primitive because $|x + 1| = 7$:

$$(x+1)^2 = x^2 + 1 \qquad (x+1)^3 = x^2 \qquad (x+1)^4 = x^2 + x + 1$$
$$(x+1)^5 = x \qquad (x+1)^6 = x^2 + x \qquad (x+1)^7 = 1.$$

The ring $E = \mathbb{Z}_3[x]/x^3 + x^2 + 2x + 1$

$E = \mathbb{Z}_3[x]/x^3 + x^2 + 2x + 1$ is a field.

$f(x) = x^3 + x^2 + 2x + 1$ is irreducible because it is cubic that has no zeros in $\mathbb{Z}_3$

$$f(0) = 1 \not\equiv_3 0 \qquad f(1) = 5 \not\equiv_3 0 \qquad f(2) = 17 \not\equiv_3 0.$$

$\chi(E) = 3$ and $|E| = 3^3 = 27$.

$-x$ is not primitive in E.

Indeed, the size of the multiplicative group E^* of E is $27 - 1 = 26 = 2 \cdot 13$. So, $-x$ is not primitive $\Leftrightarrow$ $(-x)^2 = 1$ or $(-x)^{13} = 1$. Direct computations show that

$$(-x)^2 = x^2 \neq 1 \quad \text{but} \quad (-x)^{13} = 1.$$

The ring $E = \mathbb{Z}_3[x]/x^3 + x^2 + 2x + 1$

$(x+1)^{-1} = x^2 + 2$ *in* E.

$ax^2 + bx + c \in E$ with $a, b, c \in \mathbb{Z}_3$ is a general form of an element in E. Then

$$\begin{aligned}(ax^2 + bx + c)(x+1) &= ax^3 + (a+b)x^2 + (c+b)x + c \\ &= a(2x^2 + x + 2) + (a+b)x^2 + (c+b)x + c \\ &= x^2(2a + a + b) + x(a + b + c) + (2a + c) \\ &= 1 = x^2 \cdot 0 + x \cdot 0 + 1\end{aligned}$$

which should be 1. Hence,

$$\begin{cases} 3a + b \equiv_3 0 \\ a + b + c \equiv_3 0 \\ 2a + c \equiv_3 1 \end{cases}$$

which gives $b = 0, c = 2, a = 1$. Thus, $(x+1)^{-1} = x^2 + 2$.

Nothing to see below!

Stop scrolling down!

Ideal (should be skipped)

Definition

We say that $I \subseteq R$ is an **ideal** in R if the following holds:

(ID1) I is a subgroup of the abelian group $(R, +)$;

(ID2) for any $r \in R$ and $a \in I$, $ra \in I$.

We write $I \trianglelefteq R$ if I is an ideal in R. □

Every ring R contains at least 2 ideals:

- $\{0\}$ – **trivial ideal**;
- R – **unit ideal**.

Definition

For $a_1, \ldots, a_n \in R$ the set $\langle \mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{n} \rangle = \{r_1 a_1 + \ldots + r_n a_n \mid r_1, \ldots, r_n \in R\}$ is an ideal, called the **ideal generated by** $a_1, \ldots, a_n$.

Definition

An ideal $I = \langle a \rangle$ is called **principal**.

Principal ideal domains (should be skipped)

Definition

A ring R is called the **principal ideal domain** (PID) if every ideal in R principal.

Theorem

Every ideal in $\mathbb{Z}$ is principal.

- If $I = \{0\}$, then $I = \langle 0 \rangle$.
- Otherwise, let n be the least positive number in I.
- It is easy to check that $I = \langle n \rangle$.

Theorem

Every ideal in $F[x]$ is principal.

- If $I = \{0\}$, then $I = \langle 0 \rangle$.
- If I contains a nontrivial constant, then $I = \langle 1 \rangle = F[x]$.
- Otherwise, let $f(x)$ be the monic polynomial of the least degree in I.
- It is easy to check that $I = \langle f(x) \rangle$.

Ideals in $F[x]$ (should be skipped)

Proposition

If $f(x)$ is irreducible and $g(x) \notin \langle f(x) \rangle$, then $\langle f(x), g(x) \rangle = F[x]$.

- $\langle f(x), g(x) \rangle = \langle h(x) \rangle$ for some $h(x) \in F[x]$ that divides $f(x)$ and $g(x)$
- f is irreducible $\Rightarrow$ its divisible by polynomials like $cf(x)$ and constants c
- $cf(x)$ does not divide $g(x)$ because $g(x) \notin \langle f(x) \rangle$.
- Hence, $h(x) = c$ and $\langle h(x) \rangle = F[x]$.

Equivalence modulo I (should be skipped)

Suppose that $(R, +, \cdot)$ a ring and $I \trianglelefteq R$.

Definition (a binary relation $\equiv_I$ on R)

We say that $a, b \in R$ are **equivalent modulo I** and write $a \equiv_I b$ if $b - a \in I$.

$\equiv_I$ is an equivalence relation on R.

(R) $a \equiv_I a$ for every $a \in R$.

(S) For every $a, b \in R$ we have

$$a \equiv_I b \quad \Rightarrow \quad b - a \in I \quad \Rightarrow \quad a - b \in I \quad \Rightarrow \quad b \equiv_I a.$$

(T) For every $a, b, c \in R$ we have

$$\begin{array}{c} a \equiv_I b \\ b \equiv_I c \end{array} \quad \Rightarrow \quad \begin{array}{c} b - a \in I \\ c - b \in I \end{array} \quad \Rightarrow \quad (c - b) + (b - a) = c - a \in I \quad \Rightarrow \quad a \equiv_I c.$$

$[a] = a + I$ – the equivalence class of $a \in R$.

$$[a] = \{b \in R \mid a \equiv_I b\} = \{b \in R \mid b - a \in I\} = \{b \in R \mid b \in a + I\} = a + I.$$

The set of all equivalence classes $R/I = \{a + I \mid a \in R\}$ is a partition of R.

Arithmetic of congruences

For $a+I$ and $b+I$ in R/I define

$$(\mathrm{a}+\mathrm{I})+(\mathrm{b}+\mathrm{I})=(a+b)+I,$$

$$(\mathrm{a}+\mathrm{I})\cdot(\mathrm{b}+\mathrm{I})=(a\cdot b)+I.$$

Proposition

The defined above operations $+$ and $\cdot$ are well defined on R/I, i.e., do not depend on a choice of coset representatives.

By definition, $\begin{array}{c} a+I=a'+I \\ b+I=b'+I \end{array} \quad \Leftrightarrow \quad \begin{array}{c} a'-a\in I \\ b'-b\in I \end{array}$

But then $(a'+b')-(a+b)=(a'-a)+(b'-b)\in I$ and hence,

$$(a+I)+(b+I)=(a'+I)+(b'+I).$$

Similarly, $b'(a'-a)-a(b'-b)=b'a'-ab\in I$ and hence,

$$(a+I)\cdot(b+I)=(a'+I)\cdot(b'+I).$$