

DELHI TECHNOLOGICAL UNIVERSITY



DEPARTMENT OF APPLIED MATHEMATICS

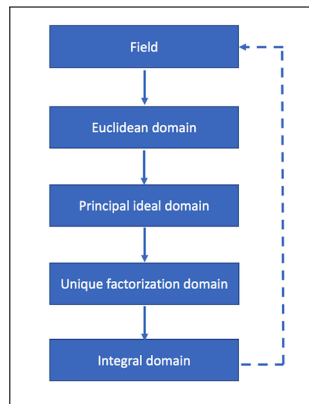
ABSTRACT ALGEBRA

MANSI YADAV 2K21/MSCMAT/30
RUMI KUMARI 2K21/MSCMAT/41

ACKNOWLEDGEMENT

In performing our project, we had to take the help and guideline of some respected persons, who deserve our greatest gratitude. The completion of this project gives us much pleasure. We should like to show our gratitude to our **Professor S.Sivaprasad Kumar**, Delhi Technological university for giving us guidelines for project through- out numerous consultations. We should also like to expand our deepest gratitude to all those who have directly and indirectly guided us in completing this project.

- Introduction
- Prerequisite
- Preliminary
- Definitions
- Theorems
- Lemmas
- Examples
- Application
- Bibliography



PRINCIPAL IDEAL DOMAIN

Introduction

Introduction In mathematics, a principal ideal domain, or PID, is an integral domain in which every ideal is principal, i.e., can be generated by a single element. More generally, a principal ideal ring is a nonzero commutative ring whose ideals are principal.

Principal ideal domains are thus mathematical objects that behave some what like the integers, with respect to divisibility: any element of a PID has a unique decomposition into prime elements (so an analogue of the fundamental theorem of arithmetic holds); any two elements of a PID have a greatest common divisor (although it may not be possible to find the using in the Euclidean algorithm). If x and y are elements of a PID without common divisors, then every element of the PID can be written in the form $ax+by=0$. Principal ideal domains are noetherian, they are integrally closed, they are unique factorization domains and Dedekind domains. All Euclidean domains and all fields are principal ideal domains.

Principal ideal domains appear in the following chain of class inclusions:

rings \subset commutative rings \subset integral domains integrally closed domains \subset unique factorization domains \subset principal ideal domains \subset Euclidean domains \subset fields \subset algebraically closed fields

PRE-REQUISITES

Before starting this project, we would like to brush up the following topics:

- Rings
- Commutative Rings
- Fields
- Zero Divisor
- Integral Domain
- Ideals
- Polynomial Rings
- Principal Ideal Rings

PRELIMINARIES

Though this project needs some prerequisites but to make the text self-contained, some basic definitions and results that we require to study this are given:

Rings

A ring R is a set with two binary operations, addition (denoted by " $a+b$ ") and multiplication (denoted by " ab "), such that for all a, b, c in R .

- 1 Closure under addition :- $a + b = b + a$
- 2 Associativity under addition :- $(a + b) + c = a + (b + c)$
- 3 Identity under addition :- There is an element 0 in R such that $a + 0 = a$.
- 4 Inverse under addition :- There is an element a'' in R such that $a + (-a) = 0$.
- 5 Associativity under multiplication :- $a(bc) = (ab)c$.
- 6 Distributive under multiplication :- $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Commutative Rings

A Commutative Ring with Unity is a Ring which is commutative under multiplication, has an identity other than 0 under multiplication, which is said to be unity of the ring.

Fields

A commutative Ring R with unity is called a Field if every non zero element is a unit, that is, every element in R has its multiplicative inverse in R .

Zero-Divisors

A nonzero element a in a commutative ring R is called a zero-divisor if there is a nonzero element b in R such that $ab = 0$.

Integral Domain

A commutative ring with unity is said to be an Integral Domain if it has no zero-divisors.

Ideals

Let $(R, +, *)$ be any ring and S be a subring of R , then S is said to be a right ideal of R if $a \in S, b \in S \implies ab \in S$,
and a left ideal of R if $a \in S; b \in S \implies ba \in S$.

Thus a non-empty subset S of R is said to be an ideal of R if:

- 1 S is a subgroup of R under addition.
- 2 For all $a \in S, b \in R$,
both ab and $ba \in S$.

Polynomial Rings

R be a commutative ring.

The set of formal symbols.

$$R[x] = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \text{ where } a_i \in R,$$

n is a non-negative integer is called the ring of polynomials over R in the indeterminate x .

Principal Ideal Domain

A Principal Ideal Domain is an integral domain R in which every ideal has $\langle a \rangle = \{ra \text{ where } r \in R\}$ for some $a \in R$ i.e, Every ideal in R is a principal ideal.

OR

A Ring R is a principal ideal domain (PID) if it is an integral domain such that every ideal of R is a principal ideal.

1- Let F be a field then $F[x]$ is a PID.

Proof:-

Let F be a field

$\implies F$ is an Integral domain

$\implies F[x]$ is also an integral domain

Let P be an idea in $F[x]$

If $P = 0$ then $P = \langle 0 \rangle$

If P is not to 0

To show: P is a principal ideal of $F[x]$

We claim that, $P = \langle g(x) \rangle$ where $g(x)$ is a polynomial in P of minimum degree.

Since $g(x) \in P \implies \langle g(x) \rangle$ is contained in P

Now, Let $f(x) \in P$, Then by division algorithm

$f(x) = g(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$

$\implies r(x) = f(x) - g(x)q(x)$

Now $f(x) \in P, g(x)q(x) \in P$ (because P is ideal)

$$\implies f(x) - g(x)q(x) \in P$$

$$\implies r(x) \in P$$

but $\deg r(x) < \deg g(x)$, So this is possible only if $r(x) = 0$

$$\implies f(x) = g(x)q(x)$$

$$\implies f(x) \in \langle g(x) \rangle$$

$$\implies P \text{ is contained in } \langle g(x) \rangle$$

$$\implies P = \langle g(x) \rangle$$

Hence P is a principal ideal generated by $g(x)$

$$\implies F[x] \text{ is a PID}$$

2-For any commutative ring R with unity $R[x]/\langle x \rangle$ is isomorphic to R

Proof:-

Define a map $Q : R[x] \rightarrow R$ as $Q(a_0 + a_1x + \dots + a_nx^n) = a_0$

To Show: Q is well defined

As

$$a_0 + a_1x + \dots + a_nx^n = b_0 + b_1x + \dots + b_nx^n$$

$$\implies a_0 = b_0$$

$$\implies Q(a_0 + a_1x + \dots + a_nx^n) = Q(b_0 + b_1x + \dots + b_nx^n)$$

To Show: Q is a Homomorphism

$$Q[(a_0 + a_1x + \dots + a_nx^n) + (b_0 + b_1x + \dots + b_mx^m)]$$

$$\implies Q[(a_0 + b_0) + (a_1 + b_1)x + \dots]$$

$$\implies a_0 + b_0$$

$$Q(a_0 + a_1x + \dots + a_nx^n) = Q(b_0 + b_1x + \dots + b_mx^m)$$

Similarly,

$$\begin{aligned} & Q[(a_0 + a_1x + \dots + a_nx^n)(b_0 + b_1x + \dots + b_mx^m)] \\ & \implies Q[(a_0b_0) + (a_1b_0 + b_1a_0)x + \dots] \\ & \implies a_0b_0 \\ & \implies Q(a_0 + a_1x + \dots + a_nx^n)Q(b_0 + b_1x + \dots + b_mx^m) \end{aligned}$$

Therefore Q is a homomorphism.

To show: Q is onto

As every $x \in R$ has preimage in $R[x]$

i.e. a polynomial with constant term x has image x in R

Therefore, By first isomorphism theorem

$$\begin{aligned} & \implies R[x]/\text{Ker}Q \text{ is isomorphic to } R \\ & \implies \text{Ker}Q = \{f(x) \in R[x] \mid Q[f(x)] = \text{constant term of } f(x) = 0\} \\ & \implies \text{Ker}Q = \{f(x) \in R[x] \mid a_0 = 0\} \\ & \implies f(x) = hx \\ & \implies \text{Ker}Q = \{f(x) = a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in R\} \\ & \implies \langle x \rangle \\ & \implies R[x]/\langle x \rangle \text{ is isomorphic to } R. \end{aligned}$$

3- Let R be a commutative ring with unity such that $R[x]$ is a PID then R is a field .

Proof:- By previous theorem

$R[x]/\langle x \rangle$ is isomorphic to R .

We claim $\langle x \rangle$ is a maximal ideal of $R[x]$

Suppose P is an ideal such that

$\langle x \rangle$ is contained in P is contained in $R[x]$

Since $R[x]$ is a PID.

$\implies P = \langle f(x) \rangle$ for some $f(x) \in R[x]$

Now $x \in \langle x \rangle$ and $\langle x \rangle$ is contained in $P = \langle f(x) \rangle$

$\implies x = f(x)g(x)$ for some $g(x) \in R[x]$

\implies either $f(x) = x$, $g(x) = 1$ (unity of $R[x]$)

OR

$$\implies f(x) = hx, g(x) = h^{-1}; h \in R$$

$$\implies f(x) = 1, g(x) = x$$

$$\text{If } f(x) = x, P = \langle f(x) \rangle \implies P = \langle x \rangle$$

$$\text{If } f(x) = hx, P = \langle f(x) \rangle \implies P = \langle hx \rangle = \langle x \rangle$$

$$\text{If } f(x) = 1, P = \langle f(x) \rangle \implies P = \langle 1 \rangle = R[x]$$

$\implies \langle x \rangle$ is maximal ideal.

Therefore $R[x]/\langle x \rangle$ is a field.

4- Every Euclidean Domain is a Principal Ideal Domain

Proof:-

Let D be a Euclidean Domain and P be a nonzero ideal of D

P is not equal to 0

Let $a \in P$ be such that $d(a)$ is minimum in P

$a \in P \implies \langle a \rangle$ is contained in P — — — — — (1)

We now show that P is contained in $\langle a \rangle$

Let $x \in P$

By division Algorithm on x and a there exist $q, r \in D$ such that

$$X = aq + r \text{ with } r = 0 \text{ or } d(r) < d(a)$$

We'll show $r = 0$

So if possible r is not equal to zero

$$\text{i.e., } r = x - qa \in P$$

$$\text{such that } d(r) < d(a)$$

which is a contradiction

$$\implies r=0$$

$$\implies x=aq$$

$$\implies x \in \langle a \rangle$$

$$\implies P \text{ is contained in } \langle a \rangle \text{ --- (2)}$$

From (1) and (2)

$$P = \langle a \rangle$$

$$\implies D \text{ is PID.}$$

5-In a PID,irreducible and primes coincide.

Proof:-

Let D be a PID

Let $a \in D$ be irreducible

To show: a is prime

As a is irreducible

therefore it is a non zero , non unit

Now let $a|bc$ ($b, c \in D$)

To show: $a = b$ or $a = c$

As $\langle a \rangle$ and $\langle b \rangle$ are ideals of D

therefore $\langle a \rangle + \langle b \rangle$ is also an ideal

As D is PID

therefore there exist $d \in D$ such that

$$\langle a \rangle + \langle b \rangle = \langle d \rangle \text{ --- (1)}$$

Now (1)

$\Rightarrow \langle a \rangle$ is contained in $\langle d \rangle$

$\Rightarrow d = a$

$\Rightarrow a = dr$ for some $r \in D$

$\Rightarrow d$ is a unit or r is unit (because a is irreducible)

Case(i)

d is a unit

therefore $\langle d \rangle = D$

$\Rightarrow \langle a \rangle + \langle b \rangle = D$ by (1)

Now $1 \in D$

therefore $1 \in \langle a \rangle + \langle b \rangle$

i.e, $1 = ax + by$ for some $x, y \in D$

hence $c = acx + bcy$

Now, a/acx

Also a/bc

$\Rightarrow a/bcy$

therefore $a/(acx + bcy)$

i.e, a/c

Case(ii)

r is a unit

\therefore exist r^{-1} such that rr^{-1}

Now $a = dr$

$$\implies r^{-1} = d$$

$$\implies ar^{-1} = d$$

$$\implies \langle d \rangle \text{ is contained in } \langle a \rangle$$

$$\therefore \langle d \rangle = \langle a \rangle$$

$$\therefore (1) \text{ becomes } \langle a \rangle + \langle b \rangle = \langle a \rangle$$

$$\therefore \langle b \rangle \text{ is contained in } \langle a \rangle$$

$$\therefore a/b$$

Conversely:-

Let a be prime

To show:- a is irreducible

Since ' a ' be a prime element

$$\therefore a = bc \quad (a/a = a/bc)$$

$$\implies a/b \text{ OR } a/c \quad (a \text{ is prime})$$

To show: either b is a unit or c is a unit

Now as a/b

$$\implies b = at \text{ for some } t \in D$$

Now $b : 1 = b = at$

$$b.1 = (bc)t \text{ (because } a = bc)$$

$$b.1 = b(ct)$$

$$1 = ct$$

$\implies c$ is a unit.

$\therefore a$ is irreducible.

6-In a PID $\langle p \rangle$ is maximal iff p is irreducible.

Proof:-

Let D be a PID and $p \in D$; p is non zero

First let $\langle p \rangle$ is maximal

To show :- p is irreducible.

p is non zero (given)

If p was a unit, then $\langle p \rangle = D$, which is not possible
 $\implies p$ is non-unit.

Now let $p = bc$ ($b, c \in D$)

To Show: b is a unit or c is a unit.

Since $p = bc$

$p \in \langle b \rangle$ which is contained in D as $\langle p \rangle$ is maximal
we must have

$$\langle b \rangle = \langle p \rangle$$

or,

$$\langle b \rangle = D$$

Case (i)

$$\langle b \rangle = \langle p \rangle$$

$$b \in \langle p \rangle$$

$$\therefore b = pr \text{ for some } r \in D$$

$$\therefore p = (pr)c = p(rc)$$

$$\therefore p(1 - rc) = 0$$

$$p = 0 \text{ or } 1 - rc = 0 \text{ (} D \text{ is I.D.)}$$

Also, p is non zero

$$1 - rc = 0$$

That is $rc = 1$

$\therefore c$ is a unit.

Case(ii) $\langle b \rangle = D$ Then b is a unit. Conversely,

Let p be irreducible

To show $\langle p \rangle$ is maximal

If $\langle p \rangle = D$, then p is a unit (not possible, as an irreducible is non unit)

$\therefore \langle p \rangle$ is not equal to D .

Now let $\langle p \rangle$ is contained in $\langle b \rangle$ is contained in $\langle D \rangle$.

Note:- (As D is PID therefore every ideal is of the form $\langle b \rangle$)

To show $\langle b \rangle = \langle p \rangle$

or $\langle b \rangle = D$

$p \in \langle p \rangle$ which is contained in $\langle b \rangle$

$\therefore p = br$ for some $r \in D$.

As p is irreducible

b is a unit OR r is a unit.

Case (i) b is a unit

Then $\langle b \rangle = D$

Case (ii) r is a unit \therefore there exist $r^{-1} \in D$ such that $rr^{-1} = 1$

Now $p = br \implies pr^{-1} = b$

$\implies b \in \langle p \rangle$

$\implies \langle b \rangle$ is contained in $\langle p \rangle$

\therefore We have $\langle b \rangle = \langle p \rangle$

Thus p is a maximal ideal of D .

7 In a PID p is prime iff $\langle p \rangle$ is a prime ideal.

Proof: Given p is prime

To show $\langle p \rangle$ is a prime ideal.

As p is non unit

$\therefore \langle p \rangle$ is not equal to R .

Now let $ab \in \langle p \rangle$

To show- $a \in \langle p \rangle$ or $b \in \langle p \rangle$

As $ab \in \langle p \rangle$

$\implies p \mid ab$

$\implies p \mid a$

or, $p = b$ (because p is prime)

$\implies a \in \langle p \rangle$.

or $b \in \langle p \rangle$

Conversely,

Let $\langle p \rangle$ be a prime ideal.

To show p is prime

Clearly, p is non unit

Let $p \nmid ab$

To show $p \nmid a$ or $p \nmid b$

$\therefore ab \in \langle p \rangle$

$\therefore a \in \langle p \rangle$

or, $b \in \langle p \rangle$ (because p is prime)

That is $p = a$ or, $p = b$.

That is $p = a$ or $p = b$.

Lemma

1 In a PID D , $a = b$ iff $\langle b \rangle$ is contained in $\langle a \rangle$

Proof: $a = b$ iff there exist $x \in D$

such that $b = ar$

iff $b \in \langle a \rangle$.

iff $\langle b \rangle$ contained in $\langle a \rangle$

2 In a PID D , u is a unit iff $\langle u \rangle = D$

Proof: u is a unit iff there exist $u^{-1} \in D$ such that $uu^{-1} = 1$

iff $u = 1$,

iff $\langle 1 \rangle$ contained in $\langle u \rangle$,

iff D is contained in $\langle u \rangle$

3 In a PID , any strictly increasing chain of ideals P_1 is contained in P_2 is contained in P_3 and so on must be finite in Length.

Proof: Let R be a PID.

Let P_1 is contained in P_1 and P_2 is contained in P_3 and so on be a chain of strictly increasing ideals in R

Let P^* be the union of all the ideals in this chain.

First we'll prove P^* is an ideal

Let $P^* = \cup P_k$

To show: P^* is an ideal

(i) Let $x, y \in P^*$

$\implies x, y \in \text{Union of } P_k$

$\implies x \in P_m$ and $y \in P_n$ for

some m, n Let m less than equal to n

$\implies x, y \in P_n$

$\implies x - y \in P_n$

$\implies x - y \in P^*$

(ii) Let $x \in P^*$ and $r \in R$

$\implies x \in \text{union of } P_k$

$\implies x \in P_n$ for some n

$\implies xr, rx \in P_n$

$\implies xr, rx \in \text{union of } P_k$

$\implies xr, rx \in P^*$

$\implies P^*$ is an ideal.

Since R is a PID $\implies P^*$ is a principal ideal.

\implies there exist $a \in R$ such that $P^* = \langle a \rangle$

As $a \in \langle a \rangle \implies a \in P^*$

$\implies a \in \text{union of } P_{k'}\text{'s}$

$\implies a \in P_m$ for some m

$\implies a \in P_m$

$\implies P^*$ is contained in P_m and P_m is contained in P^*

$\implies P^* = P_m$

$\implies \text{union of } P_{k'}\text{'s} = P_m$

$\implies P_1$ is contained P_2 and P_2 is contained in P_3 and so on is a finite chain.

Examples

1 - Show that \mathbb{Z} is a PID.

Solution:- Clearly \mathbb{Z} is an Integral Domain

We show that every ideal of \mathbb{Z} is principal ideal

Let P be an ideal of \mathbb{Z}

If $P = 0$ then $P = \langle 0 \rangle$

If P is not equal to zero there exist $a \in P$

Let a be the smallest positive integer of P

Now, $a \in P \implies \langle a \rangle$ is contained in P

To show P is contained in $\langle a \rangle$

Let $x \in P$

Then by division algorithm there exist $q, r \in \mathbb{Z}$ such that

$x = qa + r$ where $0 \leq r < a$

Now $r = x - aq$ where $x \in P$ and $a \in P$

$\implies x - aq \in P$

$\implies r \in P$

But $r < a$ and a is the smallest positive integer of P

$$\implies r = 0$$

$$\implies x = aq \in \langle a \rangle$$

$$\implies P \text{ is contained in } \langle a \rangle$$

$$\therefore P = \langle a \rangle$$

Hence Z is a PID.

2 - $Z[x]$ is not a PID.

Solution - Let P be an ideal of $Z[x]$

$$P = \{f(x) \in Z[x] \mid f(x) \text{ is even}\}$$

If possible $Z[x]$ is a PID

$$\implies \text{Every ideal is a principal ideal}$$

$$\implies \text{there exist } h(x) \in Z[x] \text{ such that}$$

$$P = \langle h(x) \rangle$$

Now $x, 2 \in P$

$$\implies 2 = h(x)f(x)$$

$$\implies x = h(x)g(x) \text{ for}$$

some $f(x), g(x) \in Z[x]$

$$0 = \deg 2 = \deg h(x) + \deg f(x)$$

$\implies h(x)$ is a constant Polynomial

$$\text{As } 2 = h(x)f(x)$$

implies $h(x) = 2, -2$.

$\implies x = 2g(x), -g(x)$, which is not possible.

Hence $Z[x]$ is not a PID.

3 - Let R be a principal ideal domain (PID) and let P be a nonzero prime ideal in R . Show that P is a maximal ideal in R .

Solution- Since R is a PID, we can write $P = (a)$, an ideal generated by an element $a \in R$.

Since P is a nonzero ideal, the element $a \neq 0$.

Now suppose that we have,

P is contained in I is contained in R for some ideal I of R .

We can write $I = (b)$ for some b since R is a PID.

The element $a \in (a) \subset (b)$ and so there is an element $c \in R$ such that $a = bc$.

Since $a = bc$ is in the prime ideal P .

we have either $b \in P$ or $c \in P$.

If $b \in P$, then it follows that $I = (b)$, and hence $P = I$.

If $c \in P = (a)$, then we have $d \in R$ such that $c = ad$.

Then we have,

$a = bc = bad$ and since R is a domain,

we have, $1 = bd$.

This yields that b is a unit

and hence $I = (b) = R$.

In summary, we observe that whenever we have P , we have either $I = P$ or $I = R$. Thus P is a maximal ideal.

4 - Prove that a quotient ring of a PID by a prime ideal is a PID.

Solution- Let P be a prime ideal of a PID R .

It follows from previous example that the ideal P is maximal.

Thus the quotient R/P is a field.

The only ideals of the field R/P are the zero ideal (0) and $R/P = (1)$ itself, which are principal. Hence R/P is a PID.

5 - Show that $Z[p\sqrt{-6}]$ is not a unique factorization domain. Why does this show that $Z[p\sqrt{-6}]$ is not a principal ideal domain?

Solution: In $Z[p\sqrt{-6}]$

Clearly $Z[p\sqrt{-6}]$ is not a PID as $\sqrt{-6}$ is irreducible which is not prime. That implies it is not a PID.

6 - Prove that $\mathbb{Z}[p\sqrt{-3}]$ is not a principal ideal domain.

Solution- To prove we use contradiction. Assume that $\mathbb{Z}[p\sqrt{-3}]$ is a principal ideal domain. As every principal ideal domain is a unique factorization domain,

we get $\mathbb{Z}[p\sqrt{-3}]$ is a unique factorization domain.

Then $4 \in \mathbb{Z}[p\sqrt{-3}]$

$$4 = 2 * 2$$

$$= (1 + \sqrt{-3})(1 - \sqrt{-3})$$

So 4 is not uniquely factorized in $\mathbb{Z}[p\sqrt{-3}]$

Now from definition of unique factorization domain

We can conclude that $\mathbb{Z}[p\sqrt{-3}]$ is not a unique factorization domain.

This is contradiction, so $\mathbb{Z}[p\sqrt{-3}]$ is not a principal ideal domain.

APPLICATION

Consider an ordinary pair of dice whose faces are labelled 1 through 6. The probability of rolling a sum of 7 is $6/36$, the probability of rolling a sum of 6 is $5/36$, and so on. Martin Gardner remarked that if one were to label the six faces of one cube with integers 1, 2, 2, 3, 3, 4 and the six faces of another cube with the integers 1, 3, 4, 5, 6, 8, then the probability of obtaining any particular sum with these dice (called Sicherman dice) is the same as the probability of rolling that sum with ordinary dice.













In this example, we show how the Sicherman labels can be derived, and that they are the only possible such labels besides 1 through 6. To do so, we utilize the fact that $Z[x]$ has the unique factorization property.













Well, there are five possibilities for the two faces:

$(5, 1), (4, 2), (3, 3), (2, 4), \text{ and } (1, 5)$.

Next we consider the product of the two polynomials created by using the ordinary dice labels as exponents:

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x)(x^6 + x^5 + x^4 + x^3 + x^2 + x)$$

						
	2	3	4	5	6	7
	3	4	5	6	7	8
	4	5	6	7	8	9
	5	6	7	8	9	10
	6	7	8	9	10	11
	7	8	9	10	11	12

						
	2	3	3	4	4	5
	4	5	5	6	6	7
	5	6	6	7	7	8
	6	7	7	8	8	9
	7	8	8	9	9	10
	9	10	10	11	11	12

Observe that we pick up the term x^6 in this product in precisely the following ways: $x^5 \cdot x^1, x^4 \cdot x^2, x^3 \cdot x^3, x^2 \cdot x^4, x^1 \cdot x^5$. Notice the correspondence between pairs of labels whose sums are 6 and pairs of terms whose products are x^6 . This correspondence is one-to-one, and it is valid for all sums and all dice—including the Sicherman dice and any other dice that yield the desired probabilities.

So, let $a_1, a_2, a_3, a_4, a_5, a_6$ and $b_1, b_2, b_3, b_4, b_5, b_6$ be any two lists of positive integer labels for a pair of cubes with the property that the probability of rolling any particular sum with these dice (let us call them weird dice) is the same as the probability of rolling that sum with ordinary dice labeled 1 through 6. Using our observation about products of polynomials, this means that

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x)(x^6 + x^5 + x^4 + x^3 + x^2 + x) = (x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6})(x^{b_1} + x^{b_2} + x^{b_3} + x^{b_4} + x^{b_5} + x^{b_6}) \quad (1)$$

The polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x$ factors uniquely into irreducibles as

$$x(x+1)(x^2+x+1)(x^2-x+1)$$

so that the left-hand side of equation (1) has the irreducible factorization. So, using theorem (Every polynomial in $Z[x]$ that is not the zero polynomial or a unit in $Z[x]$ can be written in the form $b_1 b_2 b_3 \dots b_s p_1(x) p_2(x) \dots p_m(x)$, where the b_i 's are irreducible polynomials of degree 0, and the $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore if $b_1 b_2 b_3 \dots b_s p_1(x) p_2(x) \dots p_m(x) = c_1 c_2 \dots c_t q_1(x) q_2(x) \dots q_n(x)$ where the b_i 's and c_i 's are irreducible polynomials of degree 0, and the $p_i(x)$'s and $q_i(x)$'s are irreducible polynomials of positive degree, then $s = t$, $m = n$, and, after renumbering the c_i 's and $q_i(x)$'s, we have $b_i = c_i$ for $i = 1, \dots, s$; and $p_i(x) = q_i(x)$ for $i = 1, \dots, m$.

this means that these factors are the only possible irreducible factors of $P(x) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6}$. Thus, $P(x)$ has the form $x^q(x+1)^r(x^2+x+1)^t(x^2-x+1)^u$ where $0 \leq q, r, t, u \leq 2$

To further restrict the possibilities for these four parameters, we evaluate $P(1)$ in two ways. $P(1) = 1^{a_1} + 1^{a_2} + \dots + 1^{a_5} = 6$ and $P(1) = 1^q 2^r 3^t 1^u$. Clearly, this means that $r = 1$ and $t = 1$. Evaluating $P(0)$ in two ways shows that $q \neq 0$. On the other hand, if $q = 2$ the smallest possible sum one could roll with the corresponding labels for dice would be 3. Since this violates our assumption, we have now reduced our list of possibilities for q, r, t , and u to $q = 1, r = 1, t = 1$ and $u = 0, 1, 2$. Let's consider each of these possibilities in turn.

When $u = 0$, $P(x) = x^4 + x^3 + x^3 + x^2 + x$, so the die labels are 4, 3, 3, 2, 2, 1 Sicherman die.

When $u = 1$, $P(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x$. so the die labels are 6, 5, 4, 3, 2, 1 an ordinary die.

When $u = 2$, $P(x) = x^8 + x^6 + x^5 + x^4 + x^3 + x$, so the die labels are 8, 6, 5, 4, 3, 1 the other Sicherman die.

This proves that the Sicherman dice do give the same probabilities as ordinary dice and that they are the only other pair of dice that have this property.

BIBLIOGRAPHY

1. I. N. Herstein, Topics in Algebra(2 nd Edition), Wiley Eastern Limited 2008
2. Joseph A. Gallian, Contemporary Abstract Algebra(4th Ed.), Narosa Publishing House. 1999
3. D. S. Dummit and R. M. Foote, Abstract Algebra(3rdEdition), John Wiley and Sons. 2011
4. Khanna and Bhamri, A course in Abstract Algebra(5thEdition), Vikas Publishing House. 2017