

Abstract Algebra by Pinter, Chapter 22

Amir Taaki

Abstract

Chapter 22 on Factoring Into Primes

Contents

1	A. Properties of the Relation “a” divides “b”	2
1.1	Q1	2
1.2	Q2	2
1.3	Q3	2
1.4	Q4	2
1.5	Q5	3
1.6	Q6	3
1.7	Q7	3
1.8	Q8	3
1.9	Q9	3
2	B. Properties of the gcd	3
2.1	Q1	4
2.2	Q2	4
2.3	Q3	4
2.4	Q4	5
2.5	Q5	5
2.6	Q6	5
2.7	Q7	5
3	C. Properties of Relatively Prime Integers	6
3.1	Q1	6
3.2	Q2	6
3.3	Q3	6
3.4	Q4	6
3.5	Q5	6
3.6	Q6	6
4	D. Further Properties of gcd’s and Relatively Prime Integers	7
4.1	Q1	7
4.2	Q2	7
4.3	Q3	7
4.4	Q4	7
4.5	Q5	7
4.6	Q6	8
5	E. A Property of the gcd	8
5.1	Q1	8
5.2	Q2	8
5.3	Q3	9
6	F. Least Common Multiples	9
6.1	Q1	9
6.2	Q2	9
6.3	Q3	10
6.4	Q4	10

6.5	Q5	10
6.6	Q6	10
6.7	Q7	11
6.8	Q8	11
6.9	Q9	11
7	G. Ideals in \mathbb{Z}	11
7.1	Q1	11
7.2	Q2	12
7.3	Q3	12
7.4	Q4	12
7.5	Q5	13
7.6	Q6	13
7.7	Q7	14
7.8	Q8	14
8	H. The gcd and the lcm as Operations on \mathbb{Z}	14
8.1	Q1	14
8.2	Q2	15
8.3	Q3	15
8.4	Q4	16

1 A. Properties of the Relation “ a ” divides “ b ”

1.1 Q1

If $a|b$ and $b|c$, then $a|c$.

$$a|b \implies b = ka$$

$$b|c \implies c = lb$$

$$c = l(ka) = (kl)a \implies a|c$$

1.2 Q2

$a|b$ iff $a|(-b)$ iff $(-a)|b$.

$$b = ka \iff -b = (-k)a \iff b = (-k)(-a)$$

$$a|b \iff a|(-b) \iff (-a)|b$$

1.3 Q3

$1|a$ and $(-1)|a$.

$a = 1 \cdot a = (-1) \cdot (-a)$ thus $1|a$ and $(-1)|a$

1.4 Q4

$a|0$.

$$0 = 0a \therefore a|0$$

1.5 Q5

If $c|a$ and $c|b$, then $c|(ax + by)$ for all $x, y \in \mathbb{Z}$.

$c|a$ and $c|b \implies a = kc$ and $b = lc$

$$\begin{aligned} ax + by &= kcx + lcy = c(kx + ly) \\ &\implies c|(ax + by) \end{aligned}$$

1.6 Q6

If $a > 0$ and $b > 0$ and $a|b$, then $a \leq b$.

Let $b = ka$

$k \neq 0$ because $0a = 0 = b$ but $b > 0$

If $k < 0$ then $-k > 0$ or $-k \geq 1 \implies 1 \leq -ka = -b$ which is a contradiction since $b > 0$.

Thus $k > 0$

$$\begin{aligned} 0 &< k \\ 1 &\leq k \\ a &\leq ka = b \end{aligned}$$

1.7 Q7

$a|b$ iff $ac|bc$, when $c \neq 0$.

$bc = kac \implies b = ka$ by the cancellation property.

1.8 Q8

If $a|b$ and $c|d$, then $ac|bd$.

$$b = ka \quad d = lc$$

$$bd = (ka)(lc) = (kl)ac$$

1.9 Q9

Let p be a prime. If $p|a^n$ for some $n > 0$, then $p|a$.

$$a^n = (p_1 \cdots p_r)(p_1 \cdots p_r)(p_1 \cdots p_r)$$

$$p|a^n \implies a^n = kp$$

Since a^n factors uniquely $\implies p|a$

2 B. Properties of the gcd

Prove the following, for any integers a, b , and c . For each of these problems, you will need only the definition of the gcd.

2.1 Q1

If $a > 0$ and $a|b$, then $\gcd(a, b) = a$.

$$b = ka$$

Let $t = \gcd(a, b)$ then

$$\begin{aligned} t &= ax + by \\ &= ax + (ka)y \\ &= a(x + ky) \end{aligned}$$

$$\gcd(a, b) = a$$

a is the gcd because it is the biggest divisor in a .

2.2 Q2

$\gcd(a, 0) = a$, if $a > 0$.

$$a|a \text{ and } a|0 \implies \gcd(a, 0) = a$$

2.3 Q3

$\gcd(a, b) = \gcd(a, b + xa)$ for any $x \in \mathbb{Z}$.

Let $t = \gcd(a, b)$

$$t = ka + lb$$

$$a = wu \quad b + xa = vu \text{ from } \gcd(a, b + xa)$$

$$b + xa = b + x(wu) = vu$$

$$b = u(v - xw)$$

but

$$\begin{aligned} t &= ka + lb \\ &= k(wu) + lu(v - xw) \\ &= u(kw + l(v - xw)) \end{aligned}$$

therefore it follows $u|t$

$$\text{Since } \gcd(a, b + xa) = \bar{k}a + \bar{l}(b + xa) = \bar{k}(tr) + \bar{l}(ts + x(tr))$$

Therefore t is also the gcd of a and $bx + a$.

$$\gcd(a, b) = \gcd(a, b + xa) \quad \forall x \in \mathbb{Z}$$

2.4 Q4

Let p be a prime. Then $\gcd(a, p) = 1$ or p . (Explain.)

a is a composite of primes.

That is $a = p_1 \cdots p_r$

If $a = pk$ for some k , then

1. $p|p$ and $p|a$.
2. for any integer u , since p is prime, u does not divide p .

Thus according to the definition $\gcd(a, p) = p$

Otherwise $\gcd(a, p) = 1$ because p is indivisible and does not divide a .

2.5 Q5

Suppose every common divisor of a and b is a common divisor of c and d , and vice versa. Then $\gcd(a, b) = \gcd(c, d)$.

$$\gcd(a, b) > \gcd(c, d)$$

$$\implies p_1 \cdots p_i p_j \cdots p_r > p_1 \cdots p_i$$

where $p_1 \cdots p_i$ are the prime common factors of $\gcd(a, b)$ and $\gcd(c, d)$ or $\gcd(\gcd(a, b), \gcd(c, d))$.

Then this implies that a and b have common factors $p_j \cdots p_r$ which are not in c and d .

Hence $\gcd(a, b) = \gcd(c, d)$.

2.6 Q6

If $\gcd(ab, c) = 1$, then $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$.

Let $ab = (p_1 \cdots p_r)(q_1 \cdots q_s)$

$$\gcd(ab, c) = 1 \implies \forall p_i, q_j \quad p_i \nmid c, q_j \nmid c$$

$$\forall p_i \nmid c \implies \gcd(a, c) = 1$$

Likewise for b .

2.7 Q7

Let $\gcd(a, b) = c$. Write $a = ca'$ and $b = cb'$. Then $\gcd(a', b') = 1$.

Let $\gcd(a', b') = x$

$$a = ca' = ckx$$

$$b = cb' = clx$$

$$\gcd(a, b) = cx$$

but $\gcd(a, b) = c \implies x = 1$

$$\therefore \gcd(a', b') = 1$$

3 C. Properties of Relatively Prime Integers

3.1 Q1

From theorem 3,

$$\gcd(a, b) = ra + sb \text{ for some integers } r \text{ and } s$$

But $a \perp b$, so $\gcd(a, b) = 1$. That is,

$$ra + sb = 1$$

3.2 Q2

$$\gcd(a, c) = 1 \implies a \perp c \implies a \nmid c$$

But $c \mid ab$ so $ab = ch$ for some integer h . And $\gcd(a, c) = 1$

$$\implies ka + lc = 1$$

$$\implies kab + lcb = b$$

However $ab = ch$, so

$$kch + lcb = b$$

$$c(kh + lb) = b$$

Thus $c \mid b$

3.3 Q3

$$d = pa = qc$$

$$\gcd(a, c) = 1 \implies ka + lc = 1$$

$$kad + lcd = d$$

$$ka(qc) + lc(pa) = d$$

$$ac(kq + lp) = d$$

$$ac \mid d$$

3.4 Q4

$$ka + lc = 1$$

$$kab + lcb = b$$

$$k(pd) + l(qd) = b$$

$$d(kp + lq) = b$$

$$d \mid b$$

3.5 Q5

$$d = ka + lb$$

$$a = dr \quad b = ds$$

$$d = kdr + lds$$

$$= d(kr + ls)$$

$$kr + ls = 1 \implies \gcd(r, s) = 1$$

3.6 Q6

$$ka + lc = 1$$

$$hb + jc = 1$$

$$ka(hb + jc) + lc = 1$$

$$kh(ab) + (j + l)c = 1 \implies \gcd(ab, c) = 1$$

4 D. Further Properties of gcd's and Relatively Prime Integers

4.1 Q1

$$\begin{aligned}b &= ma = nc \\ka + lc &= d \\b(ka + lc) &= bd \\bka + blc &= bd \\(nc)ka + (ma)lc &= bd \\nk \cdot ac + ml \cdot ac &= bd \\ \implies ac &\mid bd\end{aligned}$$

4.2 Q2

$$\begin{aligned}b &= mac = nad \\kc + ld &= 1 \\bkc + bld &= b \\(nad)kc + (mac)ld &= b \\acd(nk + ml) &= b\end{aligned}$$

4.3 Q3

From theorem 3,

$$J = \{ua + vb : u, v \in \mathbb{Z}\}$$

J is a principal ideal of \mathbb{Z} and $J = \langle d \rangle$.

Since $x \in J$, then x is a multiple of d and so $d \mid x$.

Likewise $d \mid x \implies x \in J$ and so x is a linear combination of a and b .

4.4 Q4

Let J be a linear combination of a and b .

$t = \gcd(a, b)$ and $J = \langle t \rangle$

Thus $t = ka + lb$ but $x \mid a$ and $x \mid b$ so $x \mid t$.

But $t \mid c$, so $c \in J$ and so c is a multiple of t (which is the biggest divisor of a and b).

$$t \leq c$$

$c \mid c \implies c \mid a$ and $c \mid b$, and c is the greatest divisor of c . So $c = \gcd(a, b) = t$.

See also [here](#)

4.5 Q5

$$\forall n > 0, \text{ if } \gcd(a, b) = 1 \text{ then } \gcd(a, b^n) = 1$$

$\gcd(a, b) = 1$ means there is only the shared divisor of 1 between a and b .

That there is no $u > 1$ such that $a = xu$ and $b = yu$.

Assume $\gcd(a, b^k) = 1$, then there is no common divisor between a and b^k and also a and b . This means that a and b^{k+1} also share no prime factors, hence

$$\gcd(a, b^{k+1}) = 1$$

4.6 Q6

Suppose $\gcd(a, b) = 1$ and $c|ab$. Then there exist integers r and s such that $c = rs$, $r|a$, $s|b$, and $\gcd(r, s) = 1$.

$$\begin{aligned}a &= p_1 \cdots p_n \\ b &= q_1 \cdots q_m\end{aligned}$$

Since $\gcd(a, b) = 1$, a and b share no factors as their prime factors are unique and distinct.

$$c \mid ab \implies ab = kc$$

Since c divides ab , it consists of some number of factors of ab such that

$$c = (p_1 \cdots p_i)(q_1 \cdots q_j)$$

that divides ab .

Let $r = (p_1 \cdots p_i)$ and $s = (q_1 \cdots q_j)$.

Then $c = rs$, $r \mid a$, $s \mid b$ and $\gcd(r, s) = 1$.

5 E. A Property of the gcd

5.1 Q1

Suppose a is odd and b is even, or vice versa. Then $\gcd(a, b) = \gcd(a + b, a - b)$.

$a + b$ and $a - b$ is odd.

t is a common divisor of $a - b$ and $a + b$. Since they are both odd, then t is odd.

Sum of $a + b$ and $a - b$ is $2a$, and difference is $2b$.

Since $a + b = tx$ and $a - b = ty$, then

$$(a + b) + (a - b) = tx + ty = t(x + y)$$

Likewise

$$(a + b) - (a - b) = t(x - y)$$

Since t is odd, $t \mid 2a \implies t \mid a$, and also $t \mid b$ thus if $t = \gcd(a + b, a - b)$, then

$$\gcd(a, b) = \gcd(a + b, a - b)$$

5.2 Q2

Suppose a and b are both odd. Then $2\gcd(a, b) = \gcd(a + b, a - b)$.

a and b are both odd.

$a + b$ and $a - b$ are thus even.

t is a common divisor of $a + b$ and $a - b$. So t is even.

$$(a + b) + (a - b) = 2a = t(x + y)$$

$$(a + b) - (a - b) = 2b = t(x - y)$$

That is $2|t$ and so $t = 2\gcd(a, b)$ but $t = \gcd(a + b, a - b)$

$$2\gcd(a, b) = \gcd(a + b, a - b)$$

5.3 Q3

If a and b are both even, explain why either of the two previous conclusions are possible.

$$\begin{aligned}a &= 2n & b &= 2m \\ \gcd(a, b) &= t = 2x \\ a + b &= 2(n + m) & a - b &= 2(n - m) \\ \gcd(a + b, a - b) &= s = 2y\end{aligned}$$

$$2a = t(x + y) \quad 2b = t(x - y)$$

a and b are even, so is t .

Thus either case is true: $t \mid a$ or $t \mid 2a$.

There isn't enough information to infer whether $t = \gcd(a, b)$ or $t = 2 \gcd(a, b)$.

6 F. Least Common Multiples

6.1 Q1

Prove: The set of all the common multiples of a and b is an ideal of \mathbb{Z} .

$$I = \{n \cdot \text{lcm}(a, b) : n \in \mathbb{Z}\}$$

$$\begin{aligned}x, y \in I, x + y &= i \cdot \text{lcm}(a, b) + j \cdot \text{lcm}(a, b) = (i + j) \cdot \text{lcm}(a, b) \\ -x &= -i \cdot \text{lcm}(a, b) \in I\end{aligned}$$

because if $a \mid c$ then $a \mid -c$

Lastly let $w \in \mathbb{Z}$

$$w \cdot x = (wi) \cdot \text{lcm}(a, b)$$

and since $wi \in \mathbb{Z}$, so $w \cdot x \in I$.

So I is an ideal of \mathbb{Z} .

6.2 Q2

Prove: Every pair of integers a and b has a least common multiple.

Every ideal of \mathbb{Z} is principal.

That means there exists a generator

$$I = \{n \cdot \text{lcm}(a, b) : n \in \mathbb{Z}\} = \langle t \rangle$$

which is a least value.

By the well ordering principle $t = 1 \cdot \text{lcm}(a, b) = \text{lcm}(a, b)$.

Since $x \mid xy$ for integers $x, y \in \mathbb{Z}$ where $x \neq 0$ and $y \neq 0$, then I must contain xy and is non-trivial.

6.3 Q3

Prove $a \cdot \text{lcm}(b, c) = \text{lcm}(ab, ac)$.

$$l = \text{lcm}(ab, ac)$$

then

$$l = abx = acy$$

for some integers x and y .

So a is a factor of l

$$l = am$$

$$am = abx = acy$$

thus

$$m = \text{lcm}(b, c)$$

$$a \cdot \text{lcm}(b, c) = \text{lcm}(ab, ac)$$

6.4 Q4

If $a = a_1c$ and $b = b_1c$ where $c = \text{gcd}(a, b)$, then $\text{lcm}(a, b) = a_1b_1c$.

$$\text{lcm}(a, b) = \text{lcm}(a_1c, b_1c) = c \cdot \text{lcm}(a_1, b_1)$$

But $\text{gcd}(a, b) = c$ and $\text{gcd}(a_1c, b_1c) = c$ so $\text{gcd}(a_1, b_1) = 1$. Since there is no q such that both $q \mid a_1$ and $q \mid b_1$, then

$$\begin{aligned} \text{lcm}(a, b) &= ax = by \\ &= a_1cx = b_1cy \\ &= cm \\ m &= a_1x = b_1y \end{aligned}$$

We know that $\text{gcd}(a_1, b_1) = 1$, which means a_1 and b_1 contain unique prime factors. That is that $x = b_1$ and $y = a_1$.

$$\text{lcm}(a, b) = a_1b_1c$$

6.5 Q5

Prove $\text{lcm}(a, ab) = ab$

$$\begin{aligned} \text{lcm}(a, ab) &= a \cdot \text{lcm}(1, b) \\ &= ab \end{aligned}$$

6.6 Q6

If $\text{gcd}(a, b) = 1$ then $\text{lcm}(a, b) = ab$.

From 4,

$$a = a_1 \text{gcd}(a, b) \qquad \qquad \qquad = a_1 \cdot 1 = a_1$$

and also $b = b_1$, so

$$\begin{aligned} \text{lcm}(a, b) &= a_1b_1c \\ &= ab \cdot \text{gcd}(a, b) \\ &= ab \end{aligned}$$

6.7 Q7

If $\text{lcm}(a, b) = ab$ then $\text{gcd}(a, b) = 1$.

$$\begin{aligned}\text{lcm}(a_1c, b_1c) &= c \cdot \text{lcm}(a_1, b_1) \\ ab &= c \cdot \text{lcm}(a_1, b_1) \\ (a_1c)(b_1c) &= c \cdot \text{lcm}(a_1, b_1) \\ a_1b_1c &= \text{lcm}(a_1, b_1)\end{aligned}$$

But $\text{gcd}(a_1, b_1) = 1 \implies \text{lcm}(a_1, b_1) = a_1b_1$ so

$$\begin{aligned}a_1b_1c &= a_1b_1 \\ c &= 1 \\ \text{gcd}(a, b) &= 1\end{aligned}$$

6.8 Q8

Let $\text{gcd}(a, b) = c$. Then $\text{lcm}(a, b) = ab/c$.

$$\begin{aligned}\text{lcm}(a, b) &= \text{lcm}(a_1c, b_1c) \\ &= c \cdot \text{lcm}(a_1, b_1)\end{aligned}$$

but $\text{gcd}(a, b) = \text{gcd}(a_1c, b_1c) = c \implies \text{gcd}(a_1, b_1) = 1$ so $\text{lcm}(a_1, b_1) = a_1b_1$.

$$\begin{aligned}\text{lcm}(a, b) &= c \cdot \text{lcm}(a_1, b_1) \\ &= ca_1b_1 \\ &= (a_1c)(b_1c)/c \\ &= ab/c\end{aligned}$$

6.9 Q9

Let $\text{gcd}(a, b) = c$ and $\text{lcm}(a, b) = d$. Then $cd = ab$.

$$\begin{aligned}\text{lcm}(a, b) &= d = ab/c \\ cd &= ab\end{aligned}$$

7 G. Ideals in \mathbb{Z}

7.1 Q1

$\langle n \rangle$ is a prime ideal iff n is a prime number.

Prime ideal:

if $ab \in J$ then $a \in J$ or $b \in J$.

Let $J = \langle n \rangle$ be a prime ideal in \mathbb{Z} .

Then $J = \{nx : x \in \mathbb{Z}\}$

Let $y \in J$, then $y = nx$ and $n \in J$.

Let $J = \langle n = uv \rangle$ where n is non-prime.

Then $uv \in J$ but $u \notin J$ and $v \notin J$, so n must be prime.

7.2 Q2

Every prime ideal of \mathbb{Z} is a maximal ideal.

$\langle p \rangle \subseteq \langle a \rangle$ so $p \in \langle a \rangle$ but $\langle p \rangle \neq \langle a \rangle \implies p \neq a$ and so $p = a \cdot n$ for some $n \in \mathbb{Z}$.

But p is prime and since $\langle p \rangle \subseteq \langle a \rangle$, then $a < p$, but $a \nmid p$ and $\gcd(a, p) = 1$.

$p \in \langle a \rangle \implies p = a \cdot n$ for some $n \in \mathbb{Z}$ but $\gcd(a, p) = 1 \implies n = \pm 1$, therefore $a = \pm p$ and so $\langle a \rangle = \langle p \rangle$. Thus every prime ideal $\langle p \rangle$ of \mathbb{Z} is a maximal ideal.

7.3 Q3

For every prime number p , \mathbb{Z}_p is a field.

Prime ideal:

if $ab \in J$ then $a \in J$ or $b \in J$.

Definition of a field: a commutative ring with unity where every nonzero element is invertible.

Every field is an integral domain.

Definition of an integral domain: a commutative ring with unity having the cancellation property. That is $ab = ac \implies b = c$.

From the end of chapter 19 on quotient rings, we have J is a maximal ideal of A (proven above).

A/J is a commutative ring with unity so the coset $J+1$ is the unity of A/J since $(J+1)(J+a) = J+a$.

Now finally to prove A/J is a field we must show for every a , there exists x such that

$$(J+a)(J+x) = J+1$$

$$K = \{xa + j : x \in A, j \in J\}$$

K is an ideal, $a \in K$ because $a = 1a + 0$ and $\forall j \in J, j \in K$ because $j = 0a + j$.

K is an ideal and contains J , but also $a \notin J$ and $a \in K$ so K is bigger than J .

But J is maximal so $K = A$.

Therefore $1 \in K$ so $1 = xa + j$ for some $x \in A$ and $j \in J$, that is $1 - xa = j \in J$.

$$J+1 = J+xa = (J+x)(J+a)$$

So $J+x$ is the multiplicative inverse of $J+a$.

Thus A/J is a field.

7.4 Q4

If $c = \text{lcm}(a, b)$, then $\langle a \rangle \cap \langle b \rangle = \langle c \rangle$.

$$c = \text{lcm}(a, b)$$

$\langle c \rangle = \{n \cdot c : n \in \mathbb{Z}\}$ therefore $\langle c \rangle$ contains all the multiples of a and b .

$\langle a \rangle$ is all the multiples of a , $\langle b \rangle$ contains all the multiples of b , and $\langle a \rangle \cap \langle b \rangle$ are all the multiples of a and b .

Any $x \in \langle a \rangle \cap \langle b \rangle$ is both in $\langle a \rangle$ and $\langle b \rangle$ and so is a multiple of both a and b . Therefore $x \in \langle c \rangle$.

$$\langle a \rangle \cap \langle b \rangle = \langle c \rangle$$

7.5 Q5

Let ϕ be a homomorphism such that

$$\phi : \mathbb{Z} \rightarrow A$$

And let J be the ideal of ϕ .

Every ideal of \mathbb{Z} is principal. By the well ordering principle pick the least value $n \in J$, and let m be any element of J . By the division algorithm $m = nq + r$ where $0 \leq r < n$. Since $n \in J$ and $m \in J$, then $r = m - nq \in J$. So either $r = 0$ or $r > 0$. But n is the least value in J , so $r = 0$. So $m = nq$.

$$J = \langle n \rangle$$

$$\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$$

Since the ideal of ϕ is $\langle n \rangle$, so

$$A \cong \mathbb{Z}/\langle n \rangle$$

Every homomorphic image of \mathbb{Z} is isomorphic to \mathbb{Z}_n for some n .

7.6 Q6

Let G be a group and let $a, b \in G$. Then $S = \{n \in \mathbb{Z} : ab^n = b^na\}$ is an ideal of \mathbb{Z} .

S is an ideal of \mathbb{Z} if it satisfies the following conditions:

1. $(S, +)$ is a subgroup of $(\mathbb{Z}, +)$
2. For every $r \in \mathbb{Z}$ and every $x \in S$, the product rx is in S

Prove S is closed under addition for $x, y \in S$:

$$\begin{aligned} ab^{x+y} &= ab^x b^y = b^x ab^y \\ &= b^x b^y a \\ &= b^{x+y} a \end{aligned}$$

Prove that for any $x \in S$, that $-x \in S$:

$$\begin{aligned} ab^n &= b^na \\ b^{-n}ab^n &= a \\ b^{-n}a &= ab^{-n} \end{aligned}$$

Lastly prove that for any $r \in \mathbb{Z}$ and every $x \in S$, the product $rx \in S$.

Observe firstly that $ab^n = b^na$ and then note that $ab^{nx} = a \underbrace{b^n b^n \dots b^n}_{x \text{ times}}$. But $b^n = a^{-1}b^na$.

$$\begin{aligned} ab^{nx} &= a \underbrace{(a^{-1}b^na)}_{b^n} b^n \dots b^n \\ &= (b^na)b^n \dots b^n \\ &= (b^na)(a^{-1}b^na) \dots b^n \\ &= b^n(b^na) \dots b^n \\ &= b^{nx}a \end{aligned}$$

And so S is an ideal of \mathbb{Z} .

7.7 Q7

Let G be a group, H a subgroup of G , and $a \in G$. Then

$$S = \{n \in \mathbb{Z} : a^n \in H\}$$

is an ideal of \mathbb{Z} .

Let $x, y \in S$, then $a^{x+y} = a^x a^y \in H$ since H is a group. Also $a^x \in H \implies a^{-x} \in H$.

Finally for any $z \in \mathbb{Z}$, $a^{xz} = \underbrace{(a^x)(a^x) \cdots (a^x)}_{z \text{ times}} \in H$.

So $S = \{n \in \mathbb{Z} : a^n \in H\}$ is an ideal of \mathbb{Z} .

7.8 Q8

Prove if $\gcd(a, b) = d$, then $\langle a \rangle + \langle b \rangle = \langle d \rangle$.

Let there be homomorphisms from \mathbb{Z} onto $\langle a \rangle$ and $\langle b \rangle$ defined by

$$\phi(x) = \bar{x}$$

Then $\langle a \rangle \cong \mathbb{Z}/J$ and $\langle b \rangle \cong \mathbb{Z}/K$.

Then $\langle a \rangle + \langle b \rangle = J + K$

$$J + K = \{x + y : x \in J, y \in K\}$$

All ideals of \mathbb{Z} are principal so there exists a generator t such that $J + K = \langle t \rangle$.

But $t = x + y$ for some $x \in J$ and $y \in K$. And $x = ka$ where $k \in \mathbb{Z}$ and $y = lb$ where $l \in \mathbb{Z}$. Thus $t = ka + lb$.

Since $\gcd(a, b) = d$ and $\langle t \rangle = J + K$ is the set of linear combinations of a and b , we know from theorem 3, that $\langle t \rangle$ is an ideal and the $\gcd(a, b)$.

Thus $J + K = \langle d \rangle$ and so

$$\langle a \rangle + \langle b \rangle = \langle d \rangle$$

where $d = \gcd(a, b)$.

8 H. The gcd and the lcm as Operations on \mathbb{Z}

For any two integers a and b , let $a \star b = \gcd(a, b)$ and $a \circ b = \text{lcm}(a, b)$. Prove the following properties of these operations:

8.1 Q1

\star and \circ are associative.

First we prove $(a \star b) \star c = a \star (b \star c)$ or that $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$

$$\gcd(a, b) \implies a = a_1 r, b = b_1 r$$

$$\gcd(a, b) = r$$

$$\gcd(\gcd(a, b), c) = \gcd(r, c) \implies r = r_1 u, c = c_1 u$$

$$\gcd(\gcd(a, b), c) = u$$

Now note that $b = b_1 r = b_1 r_1 u$ so

$$\gcd(b, c) = \gcd(b_1 r_1 u, c_1 u) = u$$

and

$$\gcd(a, \gcd(b, c)) = \gcd(a_1 r_1 u, u) = u$$

so

$$(a \star b) \star c = a \star (b \star c)$$

Secondly we prove $(a \circ b) \circ c = a \circ (b \circ c)$ or that $\text{lcm}(\text{lcm}(a, b), c) = \text{lcm}(a, \text{lcm}(b, c))$

Note that $t = \text{lcm}(a, \text{lcm}(b, c))$ then $a \mid t$ and $\text{lcm}(b, c) \mid t$. And $r = \text{lcm}(b, c)$ then $b \mid r$ and $c \mid r$, but also $r \mid t \implies b \mid t$ and $c \mid t$.

Therefore $a \mid t$, $b \mid t$ and $c \mid t$.

Likewise through the same method we can conclude $\text{lcm}(\text{lcm}(a, b), c) \mid \text{lcm}(a, \text{lcm}(b, c))$ and so they are equal.

That is given they are the *least* multiple of a, b, c and so should divide the other value which is also a multiple of a, b and c .

From this we conclude they are equal.

We can also use the fact that

$$\begin{aligned} \text{lcm}(a, \text{lcm}(b, c)) &= \text{lcm}(a, 1^{\max(b_1, c_1)} \cdot 2^{\max(b_2, c_2)} \cdot 3^{\max(b_3, c_3)} \cdot 5^{\max(b_4, c_4)} \cdot 7^{\max(b_5, c_5)} \dots) \\ &= 1^{\max(a_1, b_1, c_1)} \cdot 2^{\max(a_2, b_2, c_2)} \cdot 3^{\max(a_3, b_3, c_3)} \cdot 5^{\max(a_4, b_4, c_4)} \cdot 7^{\max(a_5, b_5, c_5)} \dots \end{aligned}$$

since the max operation is associative.

8.2 Q2

There is an identity element for \circ , but not for \star (on the set of positive integers).

Let there be an identity element e for \star , then $\text{gcd}(a, e) = a \implies a \mid e$ but also $\text{gcd}(n \cdot a, e) = n \cdot a \implies n \cdot a \mid e$. So every number divides e , and it contains every prime number an infinite number of times as its factor.

Thus there is no identity for $a \star b = \text{gcd}(a, b)$.

For the lcm note that

$$a \circ b = \text{lcm}(a, b) = ab / \text{gcd}(a, b)$$

For the identity operation

$$\begin{aligned} ae / \text{gcd}(a, e) &= \text{lcm}(a, e) = a \\ ae &= a \text{gcd}(a, e) \\ e &= \text{gcd}(a, e) \end{aligned}$$

So e divides all natural numbers

$$e = 1$$

8.3 Q3

Which integers have inverses with respect to \circ ?

Only 1 has an inverse because

$$\begin{aligned} \text{lcm}(a, b) &= 1 \\ \text{gcd}(a, b) &= ab / \text{lcm}(a, b) = ab \end{aligned}$$

that is

$$\begin{aligned} a &= a_1(ab) \\ &= a_1((a_1ab)b) \\ &= a_1a_1 \cdots b \cdot b \end{aligned}$$

$$\implies a, b = 1$$

8.4 Q4

Prove: $a \star (b \circ c) = (a \star b) \circ (a \star c)$.

$$\begin{aligned} a \star (b \circ c) &= \gcd(a, \text{lcm}(b, c)) \\ (a \star b) \circ (a \star c) &= \text{lcm}(\gcd(a, b), \gcd(a, c)) \end{aligned}$$

Let $a = a_1fg$, $b = b_1fx$, and $c = c_1gx$.

$$\begin{aligned} \gcd(a, bc / \gcd(b, c)) &= \gcd(a, bc/x) \\ &= \gcd(a_1fg, b_1fx c_1gx/x) \\ &= fg \end{aligned}$$

$$\begin{aligned} \text{lcm}(\gcd(a, b), \gcd(a, c)) &= \gcd(a, b) \cdot \gcd(a, c) / \gcd(\gcd(a, b), \gcd(a, c)) \\ &= fg / \gcd(f, g) = fg \end{aligned}$$