Abstract Algebra by Pinter, Chapter 21

Amir Taaki

Abstract

Chapter 21 on Integers

Contents

1 A. Properties of Order Relations in Integral Domains

1.1 Q1

$$a \leq b, b \leq c \implies a \leq c$$

4 cases:

$$a < b, b = c \implies a < c$$
$$a < b, b < c \implies a < c$$
$$a = b, b = c \implies a = c$$
$$a = b, b < c \implies a < c$$

1.2 Q2

$$a \leq b \implies a + c \leq b + c$$

$$a < b \implies a + c < b + c$$
$$a = b \implies a + c = b + c$$

1.3 Q3

$$a \leq b, c \geq 0 \implies ac \leq bc$$

$$a < b, c > 0 \implies ac < bc$$
$$a < b, c = 0 \implies ac = 0 = bc$$
$$a = b, c \geq 0 \implies ac = bc$$

1.4 Q4

$$c < 0 \implies -c > 0$$
$$a < b \implies -ac < -bc$$
$$-ac + bc < 0$$
$$bc < ac$$

1.5 Q5

$$a < b$$
$$a - b < 0$$
$$\implies -b < -a$$

1.6 Q6

$$a + c < b + c \implies a + c - c < b \implies a < b$$

1.7 Q7

$$ac < bc, c > 0 \implies a < b$$

$$ac < bc$$
$$\implies 0 < bc - ac$$
$$\implies 0 < c(b - a)$$

but $c > 0 \implies b - a > 0$

$$b > a$$

1.8 Q8

$$a < b, c < d$$
$$a - b < 0, 0 < d - c$$
$$\implies a - b < d - c$$
$$\implies a + c < b + d$$

2 B. Further Properties of Ordered Integral Domains

2.1 Q1

$$c^2 \geq 0 \implies (a - b)^2 \geq 0$$
$$a^2 + b^2 \geq 2ab$$

2.2 Q2

$$ab \leq 2ab$$
$$\implies a^2 + b^2 \geq ab$$
$$(-a)^2 + b^2 = a^2 + b^2 \geq -ab$$

2.3 Q3

$$(a - b)^2 + (b - c)^2 + (c - a)^2 \geq 0$$

2.4 Q4

$$a^2 + b^2 \neq 0 \implies a \neq 0, b \neq 0$$
$$(a + b)^2 > 0 \implies a^2 + b^2 > ab$$

2.5 Q5

$$a, b > 1 \implies (a - 1) > 0, (b - 1) > 0$$
$$(a - 1)(b - 1) = ab + 1 - a - b > 0$$

2.6 Q6

$$(a-1)(b-1)(c-1) > 0$$
$$abc + a + b + c - ab - ac - bc - 1 > 0$$
$$ab + ac + bc + 1 < a + b + c + abc$$

3 C. Uses of Induction

3.1 Q1

Assume S_k is correct.

$$k^2 + 2(k+1) - 1 = (k+1)^2$$

Thus is correct.

3.2 Q2

$$S_1 : 1^3 = 1^2$$

Assume S_k is true.

S_{k+1}:

$$(1 + 2 + \cdots + k)^2 + (k+1)^3 = (1 + 2 + \cdots + k + 1)^2$$
$$(\frac{k(k+1)}{2})^2 + (k+1)^3 = (\frac{(k+1)(k+2)}{2})^2$$

```
sage: bool(((k*(k + 1)) / 2)**2 + (k + 1)**3 == ((k + 1)*(k + 2)/2)**2)
True
```

3.3 Q3

$S_1 : 0^2 < \frac{1^3}{3} < 1^2$

$S_2 : 1^2 < \frac{8}{3} = 2\frac{2}{3} < 1^2 + 2^2 = 5$

Assume S_k is true, then:

$$1^2 + \cdots + (k-1)^2 < \frac{k^3}{3}$$
$$\frac{k^3}{3} < 1^2 + \cdots + k^2$$

S_{k+1}:

$$1^2 + \cdots + k^2 < \frac{(k+1)^3}{3}$$
$$1^2 + 2^2 + \cdots + (k-1)^2 + k^2 < \frac{(k+1)^3}{3}$$

but

$$1^2 + 2^2 + \cdots + (k-1)^2 + k^2 < \frac{k^3}{3} + k^2$$
$$\frac{k^3 + 3k^2}{3} < \frac{k^3 + 3k^2 + 3k + 1}{3}$$
$$\frac{k^3}{3} < 1^2 + 2^2 + \cdots + k^2$$

$$\frac{(k+1)^3}{3} < 1^2 + 2^2 + \cdots + k^2 + (k+1)^2$$

$$\frac{k^3}{3} + (k+1)^2 < 1^2 + 2^2 + \cdots + k^2 + (k+1)^2$$

$$\frac{k^3 + 3k^2 + 3k + 1}{3} < \frac{k^3 + 3k^2 + 6k + 3}{3}$$

3.4 Q4

S_1:

$$0 < \frac{1}{4} < 1^3$$

S_k:

$$1^3 + 2^3 + \cdots + (k-1)^3 < \frac{k^4}{4} < 1^3 + 2^3 + \cdots + k^3$$

S_{k+1}:

$$1^3 + 2^3 + \cdots + (k-1)^3 < \frac{k^4}{4}$$

$$1^3 + 2^3 + \cdots + (k-1)^3 + k^3 < \frac{(k+1)^4}{4}$$

$$1^3 + 2^3 + \cdots + (k-1)^3 + k^3 < \frac{k^4}{4} + k^3$$

But $\frac{k^4}{4} + k^3 = \frac{k^4+4k^3}{4}$ and $\frac{(k+1)^4}{4} = \frac{k^4+4k^3+6k^2+4k+1}{4}$, therefore $\frac{k^4}{4} + k^3 < \frac{(k+1)^4}{4}$.

$$\implies 1^3 + 2^3 + \cdots + k^3 < \frac{(k+1)^4}{4}$$

Likewise

$$\frac{k^4}{4} < 1^3 + \cdots + k^3$$

$$\frac{(k+1)^4}{4} < 1^3 + \cdots + k^3 + (k+1)^3$$

but

$$\frac{k^4}{4} + (k+1)^3 < 1^3 + \cdots + k^3 + (k+1)^3$$

and

$$\frac{(k+1)^4}{4} = \frac{k^4 + 4k^3 + 6k^2 + 4k + 1}{4} < \frac{k^4}{4} + (k+1)^3 = \frac{k^4 + 4k^3 + 12k^2 + 12k + 4}{4}$$

$$\implies \frac{(k+1)^4}{4} < 1^3 + \cdots + (k+1)^3$$

3.5 Q5

```
sage: bool((1/6)*k*(k + 1)*(2*k + 1) + (k + 1)**2 == (1/6)*(k + 1)*(k + 1 + 1)*(2*(k + 1) + 1))
True
```

3.6 Q6

```
sage: bool((k**2/4)*(k + 1)**2 + (k + 1)**3 == (1/4)*(k + 1)**2*(k + 1 + 1)**2)
True
```

3.7 Q7

$$\begin{aligned}\frac{(n+1)!-1}{(n+1)!}+\frac{n+1}{(n+2)!} &= \frac{(n+2)!-1}{(n+2)!}\\ &= \frac{(n+2)!-(n+2)+n+1}{(n+2)!}\\ &= \frac{(n+2)!-1}{(n+2)!}\end{aligned}$$

3.8 Q8

$$n = 1$$

$$\begin{aligned}F_2F_3 - F_1F_4 &= 1 \times 2 - 1 \times 3\\ &= -1 = (-1)^1\end{aligned}$$

Assume S_k is true.

S_{k+1}:

$$\begin{aligned}F_{k+2}F_{k+3} - F_{k+1}F_{k+4} &= (F_{k+1}+F_k)F_{k+3} - F_{k+1}(F_{k+3}+F_{k+2})\\ &= F_{k+1}F_{k+3} + F_kF_{k+3} - F_{k+1}F_{k+3} - F_{k+1}F_{k+2}\\ &= F_kF_{k+3} - F_{k+1}F_{k+2}\\ &= (-1)\cdot(F_{k+1}F_{k+2} - F_kF_{k+3})\\ &= (-1)\cdot(-1)^k = (-1)^{k+1}\end{aligned}$$

4 D. Every Integral System Is Isomorphic to $\mathbb{Z}$

4.1 Q1

Ordered integral domain:

If $a < b$ then $a + c < b + c$

$$0 < 1 \implies (n-1)\cdot < n \cdot 1$$

If $a < b, b < c$, then $a < c$

$$0 < n \cdot 1$$

Since A is an integral system, every positive subset has a least element, so for $m < n, m \cdot 1 < n \cdot 1$

4.2 Q2

Injective: $h(m) = m \cdot 1 = h(n) = n \cdot 1 \implies m = n$ since in an integral system if $x \neq y$ then either $x < y$ or $x > y$, and each element of the mapping $h(n) = n \cdot 1$ is distinct.

Surjective: every element of an integral system is a multiple of 1 (page 210).

4.3 Q3

$$\begin{aligned} h(m+n) = (m+n)\cdot 1 &= 1 + \cdots + 1 \\ &= m\cdot 1 + n\cdot 1 \\ &= h(m) + h(n) \\ h(mn) &= mn\cdot 1 \\ &= mn\cdot 1^2 \\ &= (m\cdot 1)(n\cdot 1) \\ &= h(m)h(n) \end{aligned}$$

5 E. Absolute Values

5.1 Q1

$a \geq 0$ then $|a| = a$ and $|-a| = -(-a) = a$

$$\implies |-a| = |a|$$

$a < 0$ then $|a| = -a$ and $|-a| = -a$

$$\implies |-a| = |a|$$

5.2 Q2

$$a \leq |a|$$

$a \geq 0$ then $|a| = a \implies a = |a|$

$a < 0$ then $|a| = -a \implies a < |a|$

5.3 Q3

$$a \geq -|a|$$

$a \geq 0$ then $-|a| = -a \implies a > -|a|$

$a < 0$ then $-|a| = a \implies a = -|a|$

5.4 Q4

$$b > 0$$
$$|a| \leq b \iff -b \leq a \leq b$$

$a \geq 0$ then $|a| = a \implies a \leq b$ and $b > 0$, then $-b < 0$ but $a \geq 0$ so $a > -b$

$a < 0$ then $|a| = -a \implies -a \leq b$, but $a < 0$ so $a < -a$ and $a < b$. Also $-a \leq b \implies a \geq -b$

For the opposite statement that $-b \leq a \leq b \implies |a| \leq b$

$a \geq 0$ then $|a| = a$ and $a \leq b \implies |a| \leq b$

$a < 0$ then $|a| = -a$ and $-b \leq a \implies -a \leq b \implies |a| \leq b$

5.5 Q5

$$|a+b| \leq |a| + |b|$$

Let $\bar{a} = a + b$ and $\bar{b} = |a| + |b|$

$$\bar{a} = \bar{b} \implies |\bar{a}| \leq \bar{b}$$
$$|a+b| \leq |a| + |b|$$

5.6 Q6

$$|a - b| \leq |a| + |b|$$

$a \geq 0, b \geq 0$ then $|a - b| < |a| + |b|$

$a \geq 0, b < 0$ then $|a - b| = |a| + |b|$

$a < 0, b \geq 0$ then $|a - b| = |a| + |b|$

$a < 0, b < 0$ then $|a - b| < |a| + |b|$

5.7 Q7

$$|ab| = |a| \cdot |b|$$

$a \geq 0, b \geq 0$ then $|ab| = |a| \cdot |b|$

$a \geq 0, b < 0$ then $ab < 0, |ab| = -ab > 0$ and $|ab| = |a| \cdot |b|$

$a < 0, b \geq 0$: see above

$a < 0, b < 0$ then $ab > 0, |ab| = |a| \cdot |b|$

5.8 Q8

$$|a| - |b| \leq |a - b|$$

From part 5:

$$|a + b| \leq |a| + |b|$$

Substitute into a, the expression $a - b$

$$|(a - b) + b| \leq |a - b| + |b|$$

$$|a| - |b| \leq |a - b|$$

5.9 Q9

From 4, $a \leq b \implies |a| \leq b$

$$|a - b| > 0$$

From 8, $||a| - |b|| \leq |a - b|$

6 F. Problems on the Division Algorithm

6.1 Q1

$$m = qn + r \qquad 0 \leq r < n$$

$$km = k(qn + r) \qquad 0 \leq kr < kn$$

So q is quotient and kr is remainder.

6.2 Q2

$$m = qn + r \qquad 0 \le r < n$$
$$q = kq_1 + r_1 \qquad 0 \le r_1 < k$$

$$m = n(kq_1 + r_1) + r = (nk)q_1 + (nr_1 + r)$$

We must show $nr_1 + r < nk$, since this is the rule of the remainder.

Now $r_1 < k \implies k - r_1 > 0$ so $k - r_1 \ge 1$,

$$\implies n(k - r_1) \ge n$$

$$\implies n + nr_1 \le nk$$

But $r < n$ so $nr_1 + r < nk$

6.3 Q3

$$n \ne 0, m = nq + r, 0 \le r < |n|$$

$$m \ge 0 \implies m \ge (0)n$$

$$m \ge nq$$

$$m < 0, n < 0 \implies -n \ge 1$$
$$\implies (-m)(-n) \ge -m$$

Add $-mn + m$ to both sides

$$m \ge (-m)n$$

$$m < 0, n > 0 \implies mn \le m$$

In every case $m \ge nq$ where $n \ne 0$ and q is an integer.

$$m \ge nq \implies m - nq = r \ge 0$$

$|n| > 0$ so if $n \le r$ then $r - |n| \ge 0$, but $r - |n| = m - |n|(q + 1)$.

But $m - |n|(q + 1) < r$ which is impossible. So $r < |n|$

6.4 Q4

$$\begin{aligned}(nq_1 + r_1) - (nq_2 + r_2) &= n(q_1 - q_2) + (r_1 - r_2)\\ &= 0\end{aligned}$$

Assume $r_2 \ge r_1$, otherwise switch the symbols. Then $r_2 - r_1 \ge 0$

$$\implies r_2 - r_1 = n(q_1 - q_2)$$

but $r_1 - r_1 < n$ and $n > 0$, so $r_1 - r_1 = 0$

6.5 Q5

$$n(q_1 - q_2) = 0, n > 0 \implies q_1 - q_2 = 0$$

$$\begin{aligned} q_1 &= q_2 \\ r_1 &= r_2 \end{aligned}$$

6.6 Q6

$$m = nq + r \implies m = r(\operatorname{mod} n)$$

7 G. Law of Multiples

7.1 Q1

$$\begin{aligned} 1 \cdot (a+b) &= a + b = 1 \cdot a + 1 \cdot b \\ (n+1) \cdot (a+b) &= n \cdot (a+b) + a + b \\ &= n \cdot a + a + n \cdot b + b \\ &= (n+1) \cdot a + (n+1) \cdot b \end{aligned}$$

7.2 Q2

$$\begin{aligned} (1+m) \cdot a &= a + m \cdot a \\ (n+1+m) \cdot a &= (n+m+1) \cdot a = (n+m) \cdot a + a & &= n \cdot a + m \cdot a + a \\ &= (n+1) \cdot a + m \cdot a \end{aligned}$$

and vice versa

7.3 Q3

$$\begin{aligned} (1 \cdot a)b &= ab = (1 \cdot b)a \\ [(n+1) \cdot a]b &= (n \cdot a + a)b \\ &= n \cdot ab + ab \\ &= (n+1) \cdot ab \\ &= [(n+1) \cdot b]a \end{aligned}$$

7.4 Q4

$$\begin{aligned} m \cdot (1 \cdot a) &= m \cdot a \\ m \cdot [(n+1) \cdot a] &= m \cdot (n \cdot a + a) \\ &= mn \cdot a + m \cdot a \\ &= (mn + m) \cdot a \\ &= [m(n+1)] \cdot a \end{aligned}$$

7.5 Q5

$$\begin{aligned} k \cdot a &= (k \cdot 1)a \\ (k+1) \cdot a &= [(k+1) \cdot 1] \cdot a \end{aligned}$$

because $(k+1) \cdot 1 = k \cdot 1 + 1$ and $1 \cdot a = a$

7.6 Q6

$$
\begin{aligned}
(1 \cdot a)(m \cdot b) &= a(m \cdot b) = m \cdot ab \\
[(k+1) \cdot a](m \cdot b) &= (k \cdot a + a)(m \cdot b) \\
&= (k \cdot a)(m \cdot b) + a(m \cdot b) \\
&= km \cdot ab + m \cdot ab \\
&= [(k+1)m] \cdot ab
\end{aligned}
$$

8 H. Principle of Strong Induction

8.1 Q1

$$k \in K \implies k+1 \in K$$

8.2 Q2

by the statement above S_k is true, implies all of S_i is true for $i < k$ and so S_{k+1} is true.

k the integers for which S_k is true so implies with the statement above and S_n is true for every n.

By the well ordering principle $b \notin K$ is the least element. By i. $b \neq 1$ so $b > 1$ but $b - 1 > 0$ and $b - 1 \in K$.

Then by ii. $b \in K$ (contradiction).