Abstract Algebra by Pinter, Chapter 20

Amir Taaki

Abstract

Chapter 20 on Integral Domains

Contents

1 A. Characteristic of an Integral Domain

1.1 Q1

Let a be any nonzero element of A. If $n \cdot a = 0$, where $n \neq 0$, then n is a multiple of the characteristic of A.

$$n \cdot a = 0 \implies n \cdot 1 = 0$$

but $\mathrm{char}(A) \cdot 1 = 0$, so n is a multiple of the characteristic of A.

1.2 Q2

If A has characteristic zero, $n \neq 0$, and $n \cdot a = 0$, then $a = 0$.

$$n \neq 0$$
$$n \cdot a = 0$$
$$n \cdot 1 \cdot a = 0$$

but $n \cdot 1 \neq 0$ because characteristic is zero.

$$a = 0$$

by cancellation property.

1.3 Q3

If A has characteristic 3, and $5 \cdot a = 0$, then $a = 0$.

$$3 \cdot a = 0$$
$$5 \cdot a = 3 \cdot a + 2 \cdot a = 2 \cdot a$$
$$2 \cdot a = 0 \implies a = 0$$

1.4 Q4

If there is a nonzero element a in A such that $256 \cdot a = 0$, then A has characteristic 2.

$$256 = 2^8$$

characteristic is prime.

$$\mathrm{char}(A) = 2$$

1.5 Q5

If there are distinct nonzero elements a and b in A such that $125 \cdot a = 125 \cdot b$, then A has characteristic

$$125 \cdot a = 125 \cdot b$$
$$5 \times 5 \cdot 1 \cdot (a - b) = 0$$
$$a \neq b \implies a - b \neq 0$$
$$5 \cdot 1 = 0$$
$$\mathrm{char}(A) = 5$$

1.6 Q6

If there are nonzero elements a and in A such that $(a + b)^2 = a^2 + b^2$, then A has characteristic 2.

Theorem 3: $(a + b)^p = a^p + b^p$

$$(a + b)^2 = a^2 + b^2$$
$$\mathrm{char}(A) = 2$$

1.7 Q7

If there are nonzero elements a and b in A such that $10a = 0$ and $14b = 0$, then A has characteristic 2.

$$2 \times 5 \cdot 1 \cdot a = 0$$
$$2 \times 7 \cdot 1 \cdot a = 0$$
$$2 \cdot 1 \cdot (5a + 7a) = 0$$
$$\mathrm{char}(A) = 2$$

2 B. Characteristic of a Finite Integral Domain

2.1 Q1

If A has characteristic q, then q is a divisor of the order of A.

By Lagrange's theorem, any subgroup divides the group order.

$1 + \cdots + 1 = 0$ and so forms a subgroup which divides the group order. The order of this subgroup is the characteristic of A.

See this question.

2.2 Q2

If the order of A is a prime number p, then the characteristic of A must be equal to p.

From above the characteristic must divide the order, but the order is prime so the characteristic must equal p.

2.3 Q3

If the order of A is p^m , where p is a prime, the characteristic of A must be equal to p.

The characteristic is prime and divides the order, hence $\mathrm{char}(A) = p$.

2.4 Q4

$81 = 3 \times 3 \times 3 \times 3$, so by above $\mathrm{char}(A) = 3$.

2.5 Q5

If A, with addition alone, is a cyclic group, the order of A is a prime number.

$$A = \langle 1, + \rangle$$
$$\mathrm{ord}(1) = |A|$$
$$\mathrm{ord}(1) \cdot 1 = 0 = |A| \cdot 1$$

but

$$\mathrm{char}(1) \cdot 1 = 0$$

Hence $\mathrm{char}(1)||A|$ But $\mathrm{ord}(1)$ is the smallest n such that $\mathrm{ord}(1) \cdot 1 = 0$ so $\mathrm{ord}(1)| \mathrm{char}(1)$ by Lagrange, and $\mathrm{ord}(1) = |A|$

Thus $|A|$ is prime since $|A| = \mathrm{char}(1)$ which is also prime.

See this question

3 C. Finite Rings

3.1 Q1

Prove every nonzero element of A is either a divisor of zero or invertible.

$$A = \{0, 1, a_1, a_2, \dots, a_n\}$$
$$|A| = n + 2$$

$$a_i 0, a_i 1, a_i a_2, \dots, a_i a_n$$

The size of this subgroup divides $|A|$.

If its size is less than $|A|$, then there exists $a_i x = 0$ where $x \neq 0$. So a_i is a divisor of zero.

Otherwise if its size equals $|A|$, then only $a_i 0 = 0$ and so $a_i x = 1$ meaning a_i is invertible.

3.2 Q2

Prove: If $a \neq 0$ is not a divisor of zero, then some positive power of a is equal to 1.

$a \neq 0$ is not a divisor of zero $\implies \operatorname{ord}(a) = |A| \implies A = \langle a \rangle$

But $1 \in A$, so for some x, $a^x = 1$

3.3 Q3

If a is invertible, then a^{-1} is equal to a positive power of a.

If a is invertible, $ax = 0 \implies (a^{-1} \cdot a)x = 0 \implies x = 0$.

Therefore a is not a divisor of zero.

$$\operatorname{ord}(a) = |A|$$
$$A = \langle a \rangle$$

So $a^{-1} = a^k$

4 D. Field of Quotients of an Integral Domain

4.1 Q1

$$[a, b] = [r, s] \implies as = br$$
$$[c, d] = [t, u] \implies cu = dt$$

$$[a, b] + [c, d] = [ad + bc, bd]$$
$$[r, s] + [t, u] = [ru + st, su]$$

$$[ad + bc, bd] = [ru + st, su] \implies (ad + bc)su = bd(ru + st)$$
$$adsu + bcsu = bdru + bdst$$
$$as \cdot du + cu \cdot bs = br \cdot du + dt \cdot bs$$

Since $as = br$ and $cu = dt$

$$br \cdot du + dt \cdot bs = br \cdot du + dt \cdot bs$$

So

$$[a, b] + [c, d] = [r, s] + [t, u]$$

4.2 Q2

$$\begin{aligned}[a,b]\cdot[c,d] &= [ac,bd]\\ [r,s]\cdot[t,u] &= [ru,su]\end{aligned}$$

$$\begin{aligned}[ac,bd]=[rt,su] &\implies acsu = bdrt\\ as\cdot cu &= br\cdot dt\end{aligned}$$

But $as = br$ and $cu = dt$ Thus

$$[a,b]\cdot[c,d] = [r,s]\cdot[t,u]$$

4.3 Q3

$$(u,v)\sim(a,b) \text{ and } (u,v)\sim(c,d) \implies (a,b)\sim(c,d)$$

$$\begin{aligned}(u,v)\sim(a,b) &\implies av = bu\\ (u,v)\sim(c,d) &\implies cv = du\end{aligned}$$

$$\begin{aligned}v &= c^{-1}du\\ av = ac^{-1}du &= bu\end{aligned}$$

$$\begin{aligned}ad &= bc\\ (a,b) &\sim (c,d)\end{aligned}$$

4.4 Q4

$$\begin{aligned}[a,b]+([c,d]+[e,f]) &= [a,b]+[cf+de,df]\\ &= [adf+bcf+bde,bdf]\\ ([a,b]+[c,d])+[e,f] &= [ad+bc,bd]+[e,f]\\ &= [adf+bcf+bde,bdf]\end{aligned}$$

$$[a,b]+[c,d] = [c,d]+[a,b]$$

4.5 Q5

$$\begin{aligned}[a,b]\cdot([c,d]\cdot[e,f]) &= [a,b]\cdot[ce,df]\\ &= [ace,bdf]\\ ([a,b]\cdot[c,d])\cdot[e,f] &= [ac,bd]\cdot[e,f]\\ &= [ace,bdf]\end{aligned}$$

$$[a,b]\cdot[c,d] = [c,d]\cdot[a,b]$$

4.6 Q6

$$\begin{aligned}[a,b]\cdot([c,d]+[e,f]) &= [a,b]\cdot[cf+de,df]\\ &= [acf+bde,bdf]\\ [a,b]\cdot[c,d]+[a,b]\cdot[e,f] &= [ac,bd]+[ae,bf]\\ &= [acbf+bdae,bdbf]\end{aligned}$$

Both are equivalent so distributive.

4.7 Q7

$$\phi(a) = [a, 1]$$

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

$$\begin{aligned}\phi(a + b) &= [a + b, 1] \\ &= \phi(a) + \phi(b) = [a, 1] + [b, 1] \\ &= [a + b, 1]\end{aligned}$$

5 E. Further Properties of the Characteristic of an Integral Domain

5.1 Q1

$$p \cdot a = 0$$
$$n = p \cdot m + r$$

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

but $n \cdot a = 0$ and $r \neq 0$ because p does not divide n

$$r \cdot a = 0 \implies a = 0$$

5.2 Q2

Characteristic is prime and since $a \neq 0$ then the characteristic must be p.

5.3 Q3

p^m is a multiple of p. So the characteristic is p.

5.4 Q4

$$f(ab) = a^p b^p = f(a)f(b)$$
$$f(a + b) = (a + b)^p = a^p + b^p = f(a) + f(b)$$

5.5 Q5

Order is prime and group is cyclic because

$$A \cong \mathbb{Z}_p$$

For any $a \in A : p \neq 0$

$$A = \langle a \rangle$$

5.6 Q6

$$\begin{aligned}(a + b)^{p^2} &= [(a + b)^p]^p = [a^p + b^p]^p \\ &= a^{p^2} + b^{p^2}\end{aligned}$$

Assume true for $n = k$

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

$$
\begin{aligned}
(a_1 + a_2 + \cdots + a_r)^{p^n} &= [(a_1 + a_2 + \cdots) + a_r]^{p^n} \\
&= (a_1 + a_2 + \cdots)^{p^n} + a_r^{p^n} \\
&= (a_1 + a_2 + \cdots)^{p^n} + a_{r-1}^{p^n} + a_r^{p^n} \\
&= a_1^{p^n} + a_2^{p^n} + \cdots + a_r^{p^n}
\end{aligned}
$$

5.7 Q7

$1 \in A$ and $1 \in B$ $n \cdot 1 = 0$ is true both in A and B

$$\implies \text{char}(A) = \text{char}(B)$$

6 F. Finite Fields

6.1 Q1

A finite field has order prime p and so is isomorphic to the cyclic group (see E5).

That is

$$A = \langle 1, + \rangle$$

Since A is finite order, $\text{char}(A) \neq 0$

6.2 Q2

$$f(a) = a^p$$

To show injective(onto):

$$f(x) = f(y) \implies x = y$$

From 18F7, the domain of f is a field and so f is injective.

This can also be shown by

$$f(a) = a^p = f(b) = b^p$$

$$\implies a^p - b^p = 0$$

$$\implies (a-b)^p = 0$$

$$\implies a = b$$

f is injective. A has p elements, so the image of f has at least p elements. But the image of f is contained in A, so it has at most p elements.

Therefore f is surjective.