A First Course in Abstract Algebra by Fraleigh 7th Edition (Notes Part IV)

Hubert Farnsworth

July 26, 2018

1 Part IV : Rings and Fields

1.1 Section 18 : Rings and Fields

<u>**18.1 Definition**</u> A **ring** $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, which we call addition and multiplication, defined on R such that the following axioms are satisfied:

$\mathscr{R}_1$. $\langle R, + \rangle$ is an abelian group.

$\mathscr{R}_2$. Multiplication is associative.

$\mathscr{R}_3$. For all $a, b, c \in R$, the **left distributive law**, $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ and the **right distributive law** $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

<u>**18.8 Theorem**</u> If R is a ring with additive identity 0, then for any $a, b \in R$ we have

1. $0a = a0 = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.

<u>**18.9 Definition**</u> For rings R and R', a map $\phi : R \to R'$ is a **homomorphism** if the following two conditions are satisfied for all $a, b \in R$:

1. $\phi(a+b) = \phi(a) + \phi(b)$.
2. $\phi(ab) = \phi(a)\phi(b)$.

<u>**18.12 Definition**</u> An **isomorphism** $\phi : R \to R'$ from a ring R to a ring R' is a homomorphism that is one to one and onto R'. The rings R and R' are then **isomorphic**.

<u>**18.14 Definition**</u> A ring in which multiplication is commutative is a **commutative ring**. A ring with a multiplicative identity element is a **ring with unity**; the multiplicative identity element 1 is called "**unity**".

18.16 Definition Let R be a ring with unity $1 \neq 0$. An element $u \in R$ is a **unit** of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a **division ring** (or **skew field**). A **field** is a commutative division ring. A noncommutative division ring is called a "**strictly skew field**".

Definition If we have a set, together with certain specified type of algebraic structure, then any subset of this set, together with a natural induced algebraic structure that yields an algebraic structure of the same type is a substructure. (group - subgroup, ring - subring, field - subfield, etc.)

Notable Exercises

5) Compute $(2,3)(3,5)$ in $\mathbb{Z}_5 \times \mathbb{Z}_9$.

(Answer) : We use the familiar properties of $\mathbb{Z}_n$ along with the definitions given for multiplication in this section to get $2 \cdot 3 = 1$ in $\mathbb{Z}_5$ and $3 \cdot 5 = 6$ in $\mathbb{Z}_9$, so $(2,3)(3,5) = (1,6) \in \mathbb{Z}_5 \times \mathbb{Z}_9$.

15) Describe all units in $\mathbb{Z} \times \mathbb{Z}$.

(Answer) : We know that $1, -1$ are the only units in $\mathbb{Z}$ with $1 \cdot 1 = 1, (-1) \cdot (-1) = 1$. From this we see that the units in $\mathbb{Z} \times \mathbb{Z}$ are $(1,1), (-1,-1), (1,-1), (-1,1)$ (note that each unit is its own multiplicative inverse as well).

17) Describe all the units in $\mathbb{Q}$.

(Answer) : The units in $\mathbb{Q}$ are all the elements of $\mathbb{Q}^*$ (all nonzero rational numbers).

19) Describe all the units in $\mathbb{Z}_4$.

(Answer) : The units in $\mathbb{Z}_4$ are 1 and 3 with $(1)(1) = 1$ and $(3)(3) = 1$ in this ring (note that 1 and 3 as integers are relatively prime to the integer 4, which is another way to know which elements of $\mathbb{Z}_4$ are units).

31) Give an example of a ring having two elements a, b such that $ab = 0$

but neither a nor b is zero.

(Answer) : One example is the ring $M_2(\mathbb{R})$ where the zero element is the 2 by 2 matrix with all entries $0 \in \mathbb{R}$. A possible choice for a, b is

$$a = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \ , \ b = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{so that } ab = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \ .$$

33) Mark the following statements as true or false.

(Answers) :

a. Every field is also a ring. – True. The definition of a field given requires the set in question to be a ring with the few added requirements of every nonzero element having a multiplicative inverse and also commutative multiplication.

c. Every ring has at least two units. – False. Consider the ring $\mathbb{Z}_2$ with unity 1 and also 1 as the only unit.

e. It is possible for a subset of a field to be a ring but not a subfield, under the induced operations. – True. Consider the field $\mathbb{Q}$ with subset $\mathbb{Z} \subset \mathbb{Q}$. Then $\mathbb{Z}$ is a ring but not a field under the usual operations applied to both $\mathbb{Q}, \mathbb{Z}$.

g. Multiplication in a field is commutative. – True. This is required by the definition.

i. Addition in a ring is commutative. – True. This is required because of the first ring axiom.

1.2 Section 19 : Integral Domains

19.2 Definition If a, b are two nonzero elements of a ring R such that $ab = 0$, then a, b are **divisors of 0** (or **0 divisors**).

19.3 Theorem In the ring $\mathbb{Z}_n$, the divisors of 0 are precisely those nonzero elements that are not relatively prime to n.

19.4 Corollary If p is prime, then Z_p has no divisors of 0.

19.5 Theorem The cancellation laws hold in a ring R if and only if R has no divisors of 0.

19.6 Definition An **integral domain** D is a commutative ring with unity $1 \neq 0$, and containing no divisors of 0.

19.9 Theorem Every field F is an integral domain.

19.11 Theorem Every finite integral domain is a field.

19.12 Corollary If p is prime, then $\mathbb{Z}_p$ is a field.

19.13 Definition If for a ring R, a positive integer n exists such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of the ring** R. If no such positive integer exists, then R is of **characteristic** 0.

19.15 Theorem Let R be a ring with unity. If $n \cdot 1 \neq 0 \ \forall n \in \mathbb{N}$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{N}$, then the smallest such n is the characteristic of R.

Notable Exercises

3) Find all solutions of the equation $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_6$.

(Answer) : We can see that there are no solutions by plugging in the 6 elements of $\mathbb{Z}_6$ in for x in $x^2 + 2x + 2$ and finding that the result is never 0. That is, $0^2 + 2(0) + 2 = 2 \neq 0, 1^2 + 2(1) + 2 = 5 \neq 0, ...5^2 + 2(5) + 2 = 25 + 10 + 2 = 1 + 4 + 2 = 1 \neq 0$.

7) Find the characteristic of the ring $R = \mathbb{Z}_3 \times 3\mathbb{Z}$.

(Answer) : This ring is of characteristic 0. To see why, suppose that for

$(a, b) \in R$, that $n \cdot (a, b) = (0, 0)$, since the zero element of the ring is $(0, 0)$. But then this would require $n \cdot b = 0$ in $3\mathbb{Z}$. Since $3\mathbb{Z} \subset \mathbb{Z}$ this can only occur if $b = 0$, but we require some n such that $n \cdot b = 0$ for any $b \in 3\mathbb{Z}$. So we conclude that R must be of characteristic 0 because there can be no $n \in \mathbb{N}$ such that $n \cdot (a, b) = (0, 0)$ for all $(a, b) \in R$.

Find the characteristic of the ring $R = \mathbb{Z}_3 \times \mathbb{Z}_4$.

(Answer) : Note that R has unity $(1, 1)$. Then by Theorem 19.15 if we can find the smallest $n\mathbb{N}$ such that $n \cdot (1, 1) = (0, 0)$, then R must be of characteristic n (If no finite n satisfies this then we conclude R is of characteristic 0). We can compute by hand to check our work, but some thought shows that $n = lcm(3, 4) = 12$ since in this case $n \cdot (1, 1) = (12, 12) = (0, 0)$ and 12 is the least positive integer such that we have a multiple of both 3 and 4. Thus, R is of characteristic 12.

13) Let R be a commutative ring with unity and of characteristic 3. Let $a, b \in R$. Compute and simplify $(a + b)^6$.

(Answer) :

$$(a + b)^6 = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6$$

$$= a^6 + 0 + 0 + ((6)(3) + 2)a^3b^3 + 0 + 0 + b^6 = a^6 + 2a^3b^3 + b^6 \ .$$

Here we have used the fact that if $a, b \in R$, then $a^pb^q \in R$ for any $p, q \in \mathbb{N} \cup \{0\}$ and $3r = 0$ for any $r \in R$, so that $3kr = k \cdot 0 = 0$ for any integer k.

17) Mark the following statements as true or false.

(Answers) :

g. The direct product of two integral domains is also an integral domain. – False. As one counterexample, consider the direct product of integral domains $\mathbb{Z} \times \mathbb{Z}$. Here $(1, 0)(0, 1) = (0, 0)$ while $(1, 0), (0, 1)$ are nonzero elements. Therefore $\mathbb{Z} \times \mathbb{Z}$ contains zero divisors.

i. $n\mathbb{Z}$ is a subdomain of $\mathbb{Z}$. – False. We assume here that subdomain refers to a sub- integral domain, which is not easy to write in a sensible way. By definition, an integral domain must contain a unity element. But $n\mathbb{Z}$ contains a unity element only if it contains $1 \in \mathbb{Z}$, which is only true if $n = 1$. For any other n, we fail to meet the conditions defining an integral domain.

1.3 Section 20 : Fermat's and Euler's Theorems

20.1 Theorem **(Fermat's Little Theorem)** If $a \in \mathbb{Z}$ and p is a prime not dividing a, the p divides $a^{p-1} - 1$, that is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

20.2 Corollary If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any prime p.

20.6 Theorem The set G_n of nonzero elements of $\mathbb{Z}_n$ that are not 0 divisors form a group under multiplication modulo n.

Definition The function $\phi : \mathbb{N} \to \mathbb{N}$, where $\phi(n)$ is the number of positive integers less than or equal to n, is called the **Euler - phi function**.

20.8 Theorem **(Euler's Theorem)** If a is an integer relatively prime to n, then n divides $a^{\phi(n)} - 1$, that is, $a^{\phi(n)} \equiv 1 \pmod{n}$.

20.10 Theorem Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in $\mathbb{Z}_m$.

20.11 Corollary If a and m are relatively prime integers, then for any integer b, the congruence $ax \equiv b \pmod{m}$ has as solutions all integers in precisely one congruence class modulo m.

20.12 Theorem Let m be a positive integer and let $a, b \in \mathbb{Z}_m$. Let $d = gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d does divide b, the equation has exactly d solutions in $\mathbb{Z}_m$.

20.13 Corollary Let $d = gcd(a, m)$. The congruence $ax \equiv b \pmod{m}$ has a solution if and only if d divides b. When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m.

Notable Exercises

1) Find a generator for the multiplicative group of nonzero elements of the field $\mathbb{Z}_7$.

(Answer) :

$$\langle 1 \rangle = \{1\}$$

(1 is not a generator)

$$\langle 2 \rangle = \{2, 4, 1\}$$

(2 is not a generator)

$$\langle 3 \rangle = \{3, 2, 6, 4, 5, 1\} = \mathbb{Z}_7 - \{0\}$$

(3 is a generator)

$$\langle 4 \rangle = \{4, 2, 1\}$$

(4 is not a generator)

$$\langle 5 \rangle = \{5, 4, 6, 2, 3, 1\} = \mathbb{Z}_7 - \{0\}$$

(5 is a generator)

$$\langle 6 \rangle = \{6, 1\}$$

(6 is not a generator)

5) Use Fermat's Theorem to find the remainder of 37^{49} when divided by 7.

(Answer) : Here we take $a = 37$ and $p = 7$ as described in Fermat's Theorem, which applies since 7 does not divide 37. We know that $37^6 \equiv 1 \pmod{7}$. From this we have

$$37^{49} = (37^6)^8 37 \equiv (1)(37) \equiv 37 \equiv 2 \pmod{7} .$$

9) Compute $\phi(pq)$ where p and q are both primes (and ϕ is the Euler-phi function.

(Answer) : There are $pq-1$ positive integers less than pq. Since p is prime, the only positive integers k that are less than pq such that $gcd(pq, k) = p$ are the the multiples of p, and there are $q-1$ of these. Similarly there are $p-1$ multiples of q so that $gcd(pq,k) = q$. All other positive integers less than pq are relatively prime to pq. So we are left with $pq - 1 - (p-1) - (q-1) = (p-1)(q-1)$.

23) Mark the following statements as true or false.

a. $a^{p-1} \equiv 1 \pmod{p}$ for all integers a and primes p. – False. This is the result of Fermat's Theorem, without including the condition that p does not divide a. We see that indeed this condition is necessary. As a counterexample to this statement, consider prime $p = 3$ and $a = 6$, so that $p|a$. Then we should have $6^{3-1} \equiv 1 \pmod{3}$, but this is not true since $36 \equiv 0 \pmod{3}$.

g. The product of two nonunits in $\mathbb{Z}_n$ may be a unit. – False. The units in $\mathbb{Z}_n$ are precisely the positive integers less than n that are relatively prime to n. So if we have two nonunits, say a, b, then a, b are not relatively prime to n. Let $gcd(a,n) = d_1 > 1$ and $gcd(b,n) = d_2 > 1$. Consider the product $ab = kd_1d_2$ for some $k \in \mathbb{Z}$. Then $gcd(ab,n) = max\{d_1, d_2\} > 1$, so that ab is not a unit in $\mathbb{Z}_n$. (Not really confident at all in this proof).

i. Every congruence $ax \equiv b \pmod{p}$, where p is prime, has a solution. – False. This is Corollary 20.11 without the requirement that a, m (where p takes the place of m in the corollary) be relatively prime. For a counterexample consider $2x \equiv 1 \pmod{2}$, which is solvable if and only if $2|2x-1$ (where x is an integer). But $2x-1$ is odd for any integer x, so that $2x-1$ can never be divisible by 2. So we conclude that the congruence equation has no integer solutions.

1.4 Section 21 : The Field of Quotients of an Integral Domain

Let D be an integral domain. We refer to D and the subset of $D \times D$ given by $S = \{(a,b) \mid a, b \in D, b \neq 0\}$ in what follows as given here unless otherwise specified.

21.1 Definition Two elements $(a,b), (c,d) \in S$ are **equivalent**, denoted by

$(a, b) \sim (c, d)$, if and only if $ad = bc$.

21.2 Lemma The relation $\sim$ from the above definition is an equivalence relation on S.

Note : To prove this lemma, it is very important that the integral domain D is commutative (which is required by definition of integral domain).

Definition

$$[(a, b)] = \{(c, d) \in S \mid (a, b) \sim (c, d)\}.$$

21.3 Lemma Let F be the set of all equivalence classes $[(a, b)]$ for $(a, b) in S$. For $[(a, b)], [(c, d)]$ in F, the equations

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

and

$$[(a, b)][(c, d)]$$

give well defined operations of addition and multiplication on F.

21.4 Lemma The map $i : D \to F$ given by $i(a) = [(a, 1)]$ is an isomorphism of D with a subring of F.

21.5 Theorem Any integral domain D can be enlarged to (or embedded in) a field F such that every element of F can be expressed as the quotient of two elements of D. (Such a field F is a **field of quotients of** D).

21.6 Theorem Let F be a field of quotients of D and let L be any field containing D. Then there exists a map $\psi : F \to L$ that gives an isomorphism of F with a subfield of L such that $\psi(a) = a$ for $a \in D$.

21.8 Corollary Every field L containing an integral domain D contains a field of quotients of D.

21.9 Corollary Any two fields of quotients of an integral domain D are isomorphic.

Notable Exercises