Math 4108 HW2

Pengfei Zhu

January 17, 2024

Exercise 1.4 Prove the equivalence of (R9) and (R9)'?

Proof.

$\Rightarrow$ Assume (R9') holds true, want to show that (R9) also holds.

Consider any elements a, b, c in the ring R with $c \neq 0$. Assume $ca = cb$. Subtract cb from both sides:

$$ca - cb = 0$$

Factor out c on the left side:

$$c(a - b) = 0$$

Now, since $c \neq 0$, given that $a = b$ from (R9), which implies $(a - b) = 0$ Then $c(a - b) = 0$ implies that $(a - b) = 0$ Therefore, (R9) implies (R9'), that is, if R is a ring with no divisors of zero, then cancellation laws hold in R.

$\Leftarrow$ Assume (R9) holds true. We want to show that (R9') also holds. Consider any elements a, b in the ring R such that $ab = 0$, and $a \neq 0$:

Since $ab = 0$ and $a \neq 0$, multiply right side by a:

$$ab = a0$$

which implies b = 0, which satisfy cancellation. Similarly, if $b \neq 0$, multiply right side by a:

$$ab = 0b$$

which implies a = 0, which satisfy cancellation. This shows that R has no zero divisors Therefore, (R9') implies (R9). As a result, there is equivalence of (R9) and (R9)'. □

Exercise 1.5 Show that every finite integral domain is a field.

wts: the existence of (nonzero) inverses within finite integral domain

Proof. Suppose R be a finite integral domain with unity, and let r be a nonzero element of R where $r \neq 0, 1$

Consider the products $rr^1, rr^2, \ldots, rr^n$. Suppose $rr^i = rr^j$ with some i,j,$i < j$ then $r^i = r^j$ by cancellation. Then $r^i - r^j = 0$ and since $i < j$, so r^{j-i} is in R.We have $r^i(1 - r^{j-i}) = r^i - r^j = 0$. As r is non zero and R is an integral

domain so r_i is non zero. But then $1 - r^{j-i} = 0$ then $r^{j-i} = 1$. It follows that as $r^{j-i-1}r = 1$. Hence r is a unit with inverse r^{j-i-1}

Then, $1 \in R$ equals $r \cdot r^{j-i-1}$ for some i,j, implying that r is invertible. By definition, the integral domain, which is a commutative ring, that satisfies the existence of inverses is a field. □

Exercise 1.7 Let $i = \sqrt{-1}$. Show that, by contrast with Example 1.2, the ring $R = a + bi\sqrt{2} : a, b \in Z$ has group of units 1,-1.

Existence of units:

For $a + bi\sqrt{2}$, consider $(1 + 0i\sqrt{2})$, which is equivalent to 1. This is the multiplicative identity in R, and thus, 1 is a unit.

consider $(0 - 1i\sqrt{2})$, which is equivalent to -1. This is also a unit.

No other units exist:

Suppose $a + bi\sqrt{2}$ is a unit in R other than 1 and -1. This implies there exists $c + di\sqrt{2}$ such that $(a + bi\sqrt{2})(c + di\sqrt{2}) = 1$. Expanding and comparing real and imaginary parts, we get two equations:

$$ac - 2bd = 1$$
$$ad + bc = 0$$

From the second equation, we can solve for $d = -\frac{bc}{a}$. Substituting this into the first equation, we get $ac + 2b^2c = 1$. Rearranging, $ac = 1 - 2b^2c$. This implies ac is odd, but $1 - 2b^2c$ is even, leading to a contradiction. Therefore, there are no units in R other than 1 and -1. In conclusion, the group of units of is $\{1, -1\}$.

Exercise 1.13 Show that a commutative ring with unity having no proper ideals is a field

To show a ring R is a field, we need to show it has multiplicative inverse similar to last exercise.

Let R be a non-zero commutative ring with unity, and let a be any non-zero element of R, then Ra is the set of ideal R

$$Ra = \{r_1a, r_2a \dots\}$$

Let $r_1a, r_2a \in R$ then $r_1a - r_2a = (r_1 - r_2)a \in Ra$ if $r \in R$, then $r(r_1a) = (rr_1)a \in R$ As a result, Ra is an ideal. Given that R has no proper ideal, then $Ra = R$ and $1 \in R = Ra$. There exist an element b in R such that $ba = 1$. That is to say, R contains inverse of each other, so R is a field.

Exercise 1.15 (i) Show that the set K = $\{ \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} : a, b \in Q\}$ is a field with respect to matrix addition and multiplication.

To show that the set K is a field with respect to matrix addition and multiplication, we need to demonstrate that K satisfies the field axioms.

Matrix Addition:

1. **Closure under Addition:**

$$A + B = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ -3(b_1 + b_2) & a_1 + a_2 \end{pmatrix} \in K$$

2. **Associativity of Addition:** Matrix addition is inherently associative.

3. **Existence of Additive Identity:** $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the additive identity in K.

4. **Existence of Additive Inverse:** For any $A \in K$, $-A = \begin{pmatrix} -a & -b \\ 3b & -a \end{pmatrix} \in K$.

Matrix Multiplication:

1. **Closure under Multiplication:**

$$AB = \begin{pmatrix} a_1a_2 - 3b_1b_2 & a_1b_2 + b_1a_2 \\ -3(a_1b_2 + b_1a_2) & -3b_1b_2 + a_1a_2 \end{pmatrix} \in K$$

2. **Associativity of Multiplication:** Matrix multiplication is inherently associative.

3. **Existence of Multiplicative Identity:** $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the multiplicative identity in K.

4. **Existence of Multiplicative Inverse:** For any $A \in K$ (except for the zero matrix), $A^{-1} = \frac{1}{a_1^2+3b_1^2} \begin{pmatrix} a_1 & -b_1 \\ 3b_1 & a_1 \end{pmatrix} \in K$.

By showing these axioms above, the set K is a field.

(ii) Show that K is isomorphic to the field $Q(i\sqrt{3})$ defined in the previous exercise.

To show that K is isomorphic to the field $Q(i\sqrt{3})$, we need to find a bijective homomorphism between the two fields. Let's denote the elements of K as $a+b\epsilon$, where $a, b \in Q$ and ϵ is an indeterminate satisfying $\epsilon^2 = -3$.

The field K consists of matrices of the form:

$$A = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix}$$

Now, let's consider the field $Q(i\sqrt{3})$, where elements are of the form $a+bi\sqrt{3}$. We can define a mapping $\phi : K \to Q(i\sqrt{3})$ as follows:

$$\phi : A \mapsto a + bi$$

Here, i in $Q(i\sqrt{3})$ corresponds to the matrix $\begin{pmatrix} 0 & 1 \\ -3 & 0 \end{pmatrix}$ in K.

The homomorphism ϕ preserves addition and multiplication:

1. $\phi(A_1 + A_2) = \phi(A_1) + \phi(A_2)$
2. $\phi(A_1 \cdot A_2) = \phi(A_1) \cdot \phi(A_2)$

Now, let's explicitly define ϕ:

$$\phi : \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \mapsto a + bi$$

The inverse mapping ϕ^{-1} can be defined as:

$$\phi^{-1} : a + bi \mapsto \begin{pmatrix} -a & b \\ -3b & -a \end{pmatrix}$$

This establishes a bijective homomorphism between K and $Q(i\sqrt{3})$, proving that the two fields are isomorphic.

Exercise 1.17 Let $\phi : K \to L$ be a non-zero homomorphism, where K and L are fields. Show that ϕ is a monomorphism.

Proof. Given $\phi : K \to L$ is a non-zero homomorphism. We want to show that ϕ is a monomorphism.

Let a, b be arbitrary elements in K such that $\phi(a) = \phi(b)$. We need to prove that $a = b$.

Consider the equation $\phi(a) = \phi(b)$. Since ϕ is a homomorphism, it preserves the field operations, and we have:

$$\phi(a) = \phi(b) \implies \phi(a - b) \in ker\phi = \{0\}$$

Now, since ϕ is non-zero, it cannot map all elements to zero. Therefore, $\phi(a - b) = 0$ implies $a - b = 0$, and consequently, $a = b$.

This shows that if $\phi(a) = \phi(b)$, then $a = b$, proving that ϕ is injective.

Therefore, $\phi : K \to L$ is a monomorphism.

□

Exercise 1.20 What happens to the construction of Q(D) if D is a field?

From textbook and lecture, we gives a way to construct a field out of an arbitrary integral domain by let $P = D(D/\{0\}) = (a, b) : a, b \in D, b \neq 0$.Previously, we also learnt that every finite integral domain is a field, so the condition will be less restrict.

Field of Fractions (Q(D)): If D is a field, then every nonzero element in D already has a multiplicative inverse in D. Therefore, when construct $Q(D)$ (the field of fractions of D), it will essentially get back D itself because every element in D is already invertible.

Smallest Field Containing D: The statement that $Q(D)$ is the smallest field containing D means that any field containing D must also contain $Q(D)$.

Let D be a field. The field of rational functions over D, denoted $Q(D)$, is defined as the set of all rational functions:

$$Q(D) = \left\{ \frac{f(D)}{g(D)} \mid f(D), g(D) \text{ are polynomials in } D,\ g(D) \neq 0 \right\}$$

Here, $f(D)$ and $g(D)$ are polynomials with coefficients in D, and $g(D)$ is not the zero polynomial.

So, if D is already a field, then $Q(D) = D$, and there is not anything new or additional from the construction. In this case, D itself is the smallest field containing D, and $Q(D)$ is just D, namely $Q(D) \simeq D$.

Exercise 1.22 Write down the multiplication table for Z_7 , and list the inverses of all the non-zero elements.

Multiplication Table for Z_7:

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

List of Inverses in Z_7 :

Inverse of 1 is 1 (since $1 \cdot 1 \equiv 1 \pmod 7$).
Inverse of 2 is 4 (since $2 \cdot 4 \equiv 1 \pmod 7$).
Inverse of 3 is 5 (since $3 \cdot 5 \equiv 1 \pmod 7$).
Inverse of 4 is 2 (since $4 \cdot 2 \equiv 1 \pmod 7$).
Inverse of 5 is 3 (since $5 \cdot 3 \equiv 1 \pmod 7$).
Inverse of 6 is 6 (since $6 \cdot 6 \equiv 1 \pmod 7$).

9. Prove that the group of units of a commutative ring with unity is in fact a group.

Proof. Let R be a commutative ring with unity, and R^* be the set of units in R. Given R is a commutative ring, an element a in R is a unit if there exists b in R such that $ab = ba = 1$. Let's check for Group Axioms:

1. Associativity(G1): The multiplication in the ring is associative, so $(ab)c = a(bc)$ for all a, b, c in R^*.

2. Identity Element(G2): The identity element in R^* is the multiplicative identity of the ring, denoted by 1, because for any unit a in R^*, $a \cdot 1 = 1 \cdot a = a$.

3. Inverse Element(G3): For any unit a in R^*, there exists b such that $ab = ba = 1$, and b is the inverse of a.

Since R^* satisfies all the group axioms, it is indeed a group. Therefore, the group of units of a commutative ring with unity forms a group. □

10. Describe an infinite field with prime characteristic.

Take the field of fractions of polynomials in $Fp[x]$. The field $F_p(X)$ is defined as follows:

$$F_p(X) = \left\{ \frac{f}{g} \mid f, g \in F_p[x], g \neq 0 \right\}$$

This represents the rational functions in the indeterminate X with coefficients in F_p, where F_p is a synonym for Z/pZ. In other words, the elements of $F_p(X)$ are ratios of polynomials in $F_p[X]$. The field $F_p(X)$ is infinite because it contains elements like 1, X, X^2, and so on. It has a characteristic of p because it contains F_p.