Rings and Modules

Harshith Sairaj Alagandala

September 18, 2023

Selected problems from Dummit and Foote [1].

Contents

Chapter 7: Introduction to Rings

7.1: Basic definitions and examples

Let R be a ring with 1.

1: By proposition 1 (3), we have $(-1)(-1) = 1 \cdot 1 = 1$. Hence $(-1)^2 = 1$.

2: Let u be a unit of R. There exists $v \in R$ such that $uv = vu = 1$. By proposition 1 (3) we have $(-u)(-v) = uv = 1$. Similarly, $(-v)(-u) = 1$. Therefore, $-u$ is a unit.

3: Let u be a unit in S. There exists $v \in S$ such that $uv = 1$. By the inclusion i of S in R we get $i(u \cdot_S v) = (i(u)) \cdot_R (i(v)) = u \cdot_R v$ and $i(1) = 1$. So $u \cdot_R v = 1$. Similarly, $v \cdot_R u = 1$. Hence, v is a unit in R.

Consider, the subring $\mathbb{Z} \subset \mathbb{Q}$. The subring $\mathbb{Z}$ contains the identity 1. The element $2 \in \mathbb{Z}$ is not a unit in $\mathbb{Z}$, but it is a unit in $\mathbb{Q}$ as $(1/2) \cdot_R 2 = 2 \cdot_R (1/2) = 1$.

11: Simplify $(x-1)(x+1) = x^2 - x + x - 1 = x^2 - 1 = 0$. Since R is an integral domain, it has no zero devisors. Then either $x-1 = 0$ or $x+1 = 0$. Hence, $x = \pm 1$.

12: Any field F is an integral domain: a non zero element $u \in F$ is a unit so it is not a zero devisor. Let S be a subring of F such that $1 \in S$. Suppose $a, b \in S$ such that $a \cdot_S b = 0$. Then by the inclusion map, we get $a \cdot_F b = 0$, which tells us either a or b must be 0 in F. Hence, by injectivity of the inclusion map, a or b must be 0 in S.

13: **(a)**: By the commutativity of integers, $(ab)^k = a^k b^k = (a^k b) b^(k-1) = nb^(k-1)$. By taking modulo n we get $(ab)^k = 0 \mod n$. So $(\overline{ab})^k = (ab)^k \mod n = 0 \mod n = \overline{0}$. Hence, $\overline{ab}$ is nilpotent.

(b): We can represent n as a multiple of primes as $p_1^{a_1} ... p_k^{a_k}$ where p_j are primes and a_j are positive integers.

Suppose, all the prime divisors p_js of n divides a. Then $a = p_1^{b_j} ... p_k^{b_k}$ where b_k are positive integers. There exists a positive integer m such that $mb_j \geq a_j$ for all j. Then $a^m = \prod_{j=1...k} p_j^{mb_j} = \prod_{j=1...k} p_j^{a_j + (mb_j - a_j)} = \prod_{j=1...k} p_j^{a_j} \prod_{j=1...k} p_j^{(mb_j - a_j)} = n \prod_{j=1...k} p_j^{(mb_j - a_j)} = 0 \mod n$. Hence, $\overline{a}$ is nilpotent.

(c): Let $f \in R$ be a non zero element. Then there exists a $x \in X$ such that $f(x) = a$ where $a \in F$ is not zero. Since $a \in F$ it is a not a zero divisor. Hence it can not be a nilpotent element. Suppose $f^m = 0$, then $f^m(x) = (f(x))^m = a^m = 0$. This gives us a contradiction as a can not be nilpotent.

14: Let $m \in \mathbb{Z}^+$ be the smallest number such that $x^m = 0$. That means $(x^{m-1}) \neq 0$. We take $\alpha^0 = 1$ for any $\alpha \in R$.

(a): We have $x^m = x(x^{m-1}) = 0$. Then x is either zero or nilpotent as x^{m-1} is not zero.

(b): As R is commutative, $(rx)^m = r^m x^m = r^m 0 = 0$.

(c): Let $k \geq m$ be a odd number. $1 = 1+x^k = (1+x)(x^{k-1} - x^{k-2} ... + 1)$. Hence, $(1+x)$ is a unit.

(d): Let u be a unit. Then $u + x = u(1 + u^{-1}x)$, by (b) we get $u^{-1}x$ is a unit and then by (c) we get $(1 + u^{-1}x)$ is a unit. Product of units is a unit. Hence $u + x$ is a unit.

15: Let $a, b \in R$ where R is a boolean ring. Then $(a + b) = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$. Then $ab + ba = 0$. Also note $a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a$. So we get $a + a = 0$. Which means $a = -a$. Using this, $ab = -ba = b(-a) = ba$. Hence, the R is commutative.

16: Let R be a boolean ring which is an integral domain. Let $a \in R$ be a non zero element. Then $a^2 = a$ and $0 = a^2 - a = a(a - 1)$. Since R is an integral domain and a is non zero, we have $a - 1 = 0$. Hence, $a = 1$. Therefore, any non zero element is 1. Which means there are only two elements in the group, ie, 0 and 1 and $1^2 = 1$. Therefore, R is $\mathbb{Z}/2\mathbb{Z}$.

26: **(a)**: Lets look at $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$, so $\nu(1) = 0$. Also, $0 = \nu(1) = \nu(-1 \cdot -1) = 2\nu(-1)$, so $\nu(-1) = 0$. So $1, -1 \in R$.

Given non zero elements $a, b \in R$, $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$. Hence, $a + b \in R$, as $\nu(a + b) \geq 0$. For additive inverse, $\nu(-a) = \nu(-1 \cdot a) = \nu(-1) + \nu(a) = \nu(a) \geq 0$. Hence, $a \in R$. Therefore, $R \subset K$ forms an abelian group in addition.

For multiplication, $\nu(ab) = \nu(a) + \nu(b) \geq 0$ which implies $ab \in R$. Hence, multiplication is closed in R. Therefore, the injection of R in K is a ring homomorphism and R is subring of K.

(b): Let $x \in K$ be non zero. By $0 = \nu(1) = \nu(x \cdot x^{-1}) = \nu(x) + \nu(x^{-1})$, we get $\nu(x) = -\nu(x^{-1})$. Hence, atlease one of them is non negative.

(c): Let $u \in R$ be a unit, which means $\nu(u) \geq 0$ and $\nu(u^{-1}) \geq 0$. As seen above, $\nu(x) = -\nu(x^{-1})$. Hence, $\nu(x) = 0$.

7.2 Examples: polynomial rings, matrix rings,and group rings

Let R be a commutative ring with 1.

1: For (a), $p(x) + q(x) = 9x^3 - 3x^2 + 37x - 9$.
For (b), $p(x) + q(x) = x^3 + x^2 + x + 1$.
For (c), $p(x) + q(x) = x$.

For (a), $p(x)q(x) = 14x^6 - 21x^5 - 15x^3 + 144x^2 + 181x + 20$.
For (b), $p(x)q(x) = x^5 + x^3 + x$.
For (c), $p(x)q(x) = 2x^6 + 1x + 2$.

3: **(a)**: We can check that $R[[x]]$ is an abelian group in addition. And with the multiplication defined, it has a ring structure as the distributive law follows just like the polynomials. We can check that $a_0 = 1$ and $a_j = 0$ for all $j > 0$ is the identity for $R[[x]]$. Commutative follows because

$$\sum_{k=0}^{n} a_k b_{n-k} = \sum_{j=0}^{n} b_j a_{n-j}$$

(b): Let us multiply $(1 - x)$ with $1 + x + x^2 + ...$. Say the product is $\sum c_j x^j$; if $j > 0$ then $c_j = a_0 b_j + a_1 b_{j-1} = 1 - 1 = 0$. And $c_0 = 1$. Hence, the product is identity.

(c): Say the sum $\sum_{j=0}^{\infty} a_j x^j$ is a unit. Then it has an inverse, say $\sum_{j=0}^{\infty} b_j x^j$. Their product must be 1. In particular, the last term $a_0 b_0 = 1$. Hence a_0 must be a unit in R.

Say a_0 is a unit in R. Let $b_0 = a_0^{-1}$. We recursively define $b_j = -a_0^{-1} \sum_{k=1}^{j} a_k b_{j-k}$. Then we can check the product of the formal series is 1.

4: Let $\alpha = (\sum_{j=0}^{\infty} a_j x^j)$ and $\beta = (\sum_{j=0}^{\infty} b_j x^j)$. Suppose $\alpha\beta = 0$. Then $\sum_{k=0}^{j} a_k b_{j-k} = 0$. In particular, $a_0 b_0 = 0$. Since R is an integral domain, we must have either a_0 or b_0 is zero.

Now suppose the first $k - 1$ coefficients are zero for α or β. Say they are zero for α: then $0 = a_k b_0 + a_{k-1} b_1 + ... + a_0 b_k = a_k b_0$. Then either $a_k = 0$ or $b_0 = 0$. Suppose $a_k \neq 0$, then $0 = a_{k+1} b_0 + a_k b_1 + ... + a_0 b_{k+1} = a_k b_1$ gives $b_1 = 0$. Iteratively, $0 = a_{k+m} b_0 + a_{k+m-1} b_1 + ... + a_0 b_{k+m} = a_k b_m$ gives $b_m = 0$ where $m \leq k$. Hence, the first k coefficients are zero for α or β.

By induction this holds for any positive integer k. Therefore, either α or β must be zero.

8: Let (a_{ij}) and (b_{ij}) be two matrices such that $a_{ij} = 0$ when $i \geq j$ and $b_{ij} = 0$ when $i + k \geq j$ for some $k \leq n$.

Let (c_{ij}) denote their product

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Take i and j such that $i + k + 1 \geq j$.

$$c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj} = \sum_{l=1}^{i} a_{il} b_{lj} + \sum_{l=i+1}^{n} a_{il} b_{lj} = 0 + 0$$

Therefore, we have $c_{ij} = 0$ when $i + (k + 1) \geq j$.

If A is an upper triangular matrix then by inducting on the above statement, we get A^n has all its elements zero. As for any i and j we have $i + n \geq j$ in an $n \times n$ matrix.

7.3 Ring homomorphisms and Quotient rings

Let R be a ring with $1 \neq 0$.

1: Let ϕ be an homomorphism from $2\mathbb{Z}$ to $3\mathbb{Z}$. Suppose $\phi(2) = 3m$ where $m \in \mathbb{Z}$.

$$6m = \phi(2) + \phi(2) = \phi(2 + 2) = \phi(2 \cdot 2) = \phi(2) \cdot \phi(2) = 9m^2$$

So $6m - 9m^2 = 0$ and $3m(2 - 3m) = 0$. Since $\mathbb{Z}$ is an integral domain, we have $m = 0$. As $\phi(2) = \phi(0) = 0$, ϕ is not an isomorphisms.

2: By proposition 4, the units of $\mathbb{Z}[x]$ are the units of $\mathbb{Z}$ which is the singletonset $\{1\}$. Similarly, the units of $\mathbb{Q}[x]$ are the units of $\mathbb{Q}$. Every non zero element is a unit in $\mathbb{Q}$.

Let ϕ be an isomorphism from $\mathbb{Q}[x]$ to $\mathbb{Z}[x]$. Note $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$, either $\phi(1) = 0$ or $\phi(1) = 1$ (as $\mathbb{Z}$ is a integral domain). Since ϕ is an isomorphism then $\phi(1)$ must be 1. Let $u \in \mathbb{Q}[x]$ be a unit, then $\phi(1) = \phi(u \cdot u^{-1}) = \phi(u) * \phi(u^{-1})$. This shows that a unit maps to a unit. Since an isomorphism is a bijection the number of units must be the same in both the rings. Which is not the case here. Hence we can not have an isomorpisms.

References

[1] David Steven Dummit and Richard M Foote. *Abstract algebra.* Vol. 3. Wiley Hoboken, 2004.