Math 103B - HW-1 (solution)

TA : Shubham Sinha

January 23, 2020

All problems are from **A first course in Abstract Algebra** by John B. Fraleigh.

Chapter 18

12. Let $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ with the usual addition and multiplication.

    Answer. We claim that R is a ring, moreover it is a field.

    Let a, b, c and d be rational number and $\alpha = a + b\sqrt{2}$ and $\beta = c + d\sqrt{2}$, then the ring operations are
    Addition : $\alpha + \beta = (a + c) + (b + d)\sqrt{2}$
    Multiplication : $\alpha \cdot \beta = (ac + 2bd) + (ad + bc)\sqrt{2}$.

    R is clearly an abelian subgroup of $\mathbb{R}$ under addition, and closed under multiplication. Hence R is a subring of $\mathbb{R}$, hence R is a commutative ring. Note that $1 \in R$, and $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$, hence 1 is the unity.

    To show that R is a field, we need to show that any non-zero $\alpha = (a + b\sqrt{2}) \in R$ has a multiplicative inverse. Let $\alpha^{-1} = \frac{a-b\sqrt{2}}{a^2-2b^2}$, we note that it is well defined (i.e $a^2 - 2b^2 \neq 0$), otherwise $a = b\sqrt{2}$ which implies $a = b = 0$ since $\sqrt{2}$ is irrational, but we took $\alpha \neq 0$.

    We finish the proof by noting that

    $$\alpha \cdot \alpha^{-1} = (a + b\sqrt{2}) \cdot \frac{a - b\sqrt{2}}{a^2 - 2b^2} = 1.$$

    □

18. Describe all units in the ring $R = \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$.

    Answer. Any element α in R can be written as $\alpha = (m, a, n)$ where $m, n \in \mathbb{Z}$ and $a \in \mathbb{Q}$. Note that $(1, 1, 1)$ is the unity of R, thus α is a unit if and only if there exists $\beta = (p, x, q)$ such that $\alpha \cdot \beta = (1, 1, 1)$ which provides us with the equations

    $$mp = ax = nq = 1. \tag{1}$$

Since m, q and n, p are integer pairs we get $n = \pm 1$ and $m = \pm 1$, and since x can be any rational number $a \in \mathbb{Q}^* = \mathbb{Q} - \{0\}$. This gives us that necessary conditions.

It is easy see that any $\alpha = (m, a, n) \in \{\pm 1\} \times \mathbb{Q}^* \times \{\pm 1\}$, we see that $\alpha^{-1} = (m, \frac{1}{a}, n)$ is the requires inverse. □

26. How many homomorphisms are there from $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$?

Answer. Observe that $e_1 = (1, 0, 0), e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$ are generator for the ring (or abelian group) $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. So any homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is determined by the values $d_i = \phi(e_i)$.

Note that $n \cdot (a, b, c) = (na, nb, nc)$ and $(a, b, c)^2 = (a^2, b^2, c^2)$. Using that property of homomorphism we see that $\phi(4e_i) = 4d_i$ (by additivity) and $\phi(4e_i) = \phi((2e_i)^2) = (2d_i)^2 = 4d_i^2$. Thus equating the two equations we get $4d_i^2 = 4d_i$ which has only two solution $d_i = 0$ or $d_i = 1$.

Moreover note that $e_i \cdot e_j = 0$ for $i \neq j$, thus $\phi(e_i \cdot e_j) = 0 = d_i d_j$ for distinct i and j.This implies at most one of the d_i's can be non-zero.

The above arguments leaves us with the following possible solutions : $(d_1, d_2, d_3) = (0, 0, 0)$ which is the zero homomorphism, $(d_1, d_2, d_3) = (1, 0, 0)$, $(d_1, d_2, d_3) = (0, 1, 0)$ and $(d_1, d_2, d_3) = (0, 0, 1)$. The latter three gives us valid (projection) homomorphisms $\phi(a, b, c) = a$, $\phi(a, b, c) = b$ and $\phi(a, b, c) = c$.

Hence there are total of **4** homomorphisms. □

28. Find all solution of equation $x^2 + x - 6 = 0$ in the ring $\mathbb{Z}_{14}$ by factoring the quadratic polynomial.

Answer. Observe that $x^2 + x - 6 = (x + 3)(x - 2)$. In the ring $\mathbb{Z}_{14}$, $a \cdot b = 0$ implies that $14|ab$, where $a, b \in 0, 1, \ldots, 13$. If either is zero then $ab = 0$, otherwise $a = 7$ and $2|b$ or vice versa. Using this description, we write down all the possible solutions :

Case 1 : $x + 3 = 0$, then $x = -3$ is a solution.
Case 2 : $(x - 2) = 0$, then $x = 2$ is a solution.
Case 3 : $(x + 3) = 7$, then $x = 4$ and note that $2|(x - 2) = 2$ thus it is a solution.
Case 4 : $(x - 2) = 7$, then $x = 9$ and note that $2|(x + 3) = 12$ thus it is a solution. □

38. Prove that $(a-b)(a+b) = a^2 - b^2$ for all a, b ina ring R if and only if R is a commutative.

Proof. ($\Longrightarrow$) : Using distributive property of ring we see that $(a - b)(a + b) = a(a + b) - b(a + b) = a^2 + ab - ba - b^2$. So by the assumption that $(a - b)(a + b) = a^2 - b^2$, we get $a^2 + ab - ba - b^2 = a^2 - b^2$ which indeed imply $ab = ba$ for any $a, b \in R$. Hence R is commutative.
($\Longleftarrow$) : If R is commutative, for any $a, b \in R$, we have $(a-b)(a+b) = a^2 + ab - ba - b^2 = a^2 - b^2$. □

Chapter 19

1 Find all solutions to the equation $x^3 - 2x^2 - 3x = 0$ in $\mathbb{Z}_{12}$.

Answer. Note that $x^3 - 2x^2 - 3x = x(x+1)(x-3)$. Solving this equation modulo 3 and 4, we get $x \equiv 0, 2 \mod 3$ and $x \equiv 0, 1, 3 \mod 4$. Thus using chinese remainder theorem, we readily see that the solutions in $\mathbb{Z}_{12}$ are $\{0, 3, 5, 8, 9, 11\}$. □

17. Mark true or false :
(a) False; since $n\mathbb{Z}$ is a subring of an integral domain ($\mathbb{Z}$).
(b) True; if any element a of a field is zero divisor (i.e $ab = 0$ for some $b \neq 0$), then $1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = 0$ which is contradictory.
(c) False; Note that $\{n, 2n, 3n, \dots\}$ is infinite, thus char of $n\mathbb{Z}$ is 0.
(d) False; If $\phi : \mathbb{Z} \to 2\mathbb{Z}$ is an isomorphism, $4\phi(1) = \phi(4) = \phi(2^2) = 4\phi(1)^2$, thus $\phi(1)$ equals 0 or 1. Since $1 \notin 2\mathbb{Z}$, $\phi(1) = 0$ which is contradiction to the assumption that ϕ is an isomorphism.
(e) True; Any ring isomorphic to an integral domain is an integral domian.
(f) True; Let e be the unity for the integral domain. Then consider the set $A = \{e, 2e, 3e, \dots\}$. Note that $n \cdot e \neq 0$ for any n, since otherwise $n \cdot a = n \cdot e \cdot a = 0$ for all elements a in the ring. Thus $|A|$ is infinite.
(h) True; Same reason as part (b).