# Math 103B
# Homework # 1 Solutions

Due on April 11th

*Professer Golsefidy*

**Prepared by: Rosemary Elliott Smith**

## Problem 1

Let $R_1, \cdots, R_n$ be rings. First assume $R_1 \times \cdots \times R_n$ is unital. Then $\exists a := (a_1, \cdots, a_n) \in R_1 \times \cdots \times R_n$ such that $\forall b \in R_1 \times \cdots \times R_n$, $a \cdot b = b \cdot a = b$. Take $b_i \in R_i$, and define $b = (0, \cdots 0, b_i, 0, \cdot, 0)$, where $b_i$ is in the $i$th component. Then $a \cdot b = (0, \cdots, 0, a_i \cdot b_i, 0, \cdots, 0) = b$, and so comparing components we see $a_i \cdot b_i = b_i$, and similarly for $b \cdot a = b \implies b_i a_i = b_i$. Therefore, $a_i \in R_i$ is the unity of $R_i$. Now let $R_i$ be unital for all $i \in \{1, \cdots, n\}$, and denote the unity of $R_i$ by $e_i$. Take $b := (b_1, \cdots, b_n) \in R_1 \times \cdots \times R_n$, and consider $(e_1, \cdots, e_n) \cdot b = (e_1 \cdot b_1, \cdots, e_n \cdot b_n) = b = (b_1 \cdot e_1, \cdots, b_n \cdot e_n) = b \cdot (e_1, \cdots, e_n)$ by the definition of unity in each $R_i$. Therefore, $(e_1, \cdots, e_n)$ is the unity of $R_1 \times \cdots \times R_n$. $\square$

## Problem 2

Let $R$ be a ring. Note that the set of units $U(R)$ is also denoted $R^\times$. Clearly, $1_R \cdot 1_R = 1_R$, so $1_R \in U(R)$, so $U(R) \neq \emptyset$. Take $a, b \in U(R)$. We know $\exists a^{-1}, b^{-1} \in R$. As $(a \cdot b) \cdot (b^{-1} a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = 1_R = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b)$, we see $a \cdot b \in U(R)$. As multiplication in the ring is associative, so too is multiplication in $U(R)$. As $1_R \cdot a = a \cdot 1_R = a$, $\forall a \in R$, and $U(R) \subseteq R$, $1_R$ is the identity of $U(R)$. Finally, if $a \in U(R)$, $\exists a^{-1} \in R$, and as $(a^{-1})^{-1} = a$, $a^{-1} \in U(R)$, and so $U(R)$ has inverses.

As $R_i$ are unital for $i \in \{1, \cdots, n\}$, by Problem 1 we know $R_1 \times \cdots \times R_n$ is unital. Let 1 denote the unity of $R_1 \times \cdots \times R_n$, and $e_i$ be the unity of $R_i$, $\forall i \in \{1, \cdots, n\}$ (note that again by Problem 1, $1 = (e_1, \cdots, e_n)$). We will show $U(R_1 \times \cdots \times R_n) = U(R_1) \times \cdots \times U(R_n)$. First take $b := (b_1, \cdots, b_n) \in U(R_1 \times \cdots \times R_n)$. Then $\exists b^{-1} := (a_1, \cdots, a_n) \in R_1 \times \cdots \times R_n$, and so $b \cdot b^{-1} = 1 = b^{-1} \cdot b \implies a_i \cdot b_i = b_i \cdot a_i = e_i$, $\forall i \in \{1, \cdots, n\}$. Therefore, $b_i \in U(R_i)$, $\forall i$, and so $b \in U(R_1) \times \cdots \times U(R_n)$. Now take $b = (b_1, \cdots, b_n) \in U(R_1) \times \cdots \times U(R_n)$. Let $a = (b_1^{-1}, \cdots, b_n^1)$. Then $a \cdot b = (b_1^{-1} \cdot b_1, \cdots, b_n^{-1} \cdot b_n) = (e_1, \cdots, e_n) = 1 = b \cdot a$, and so $b \in U(R_1 \times \cdots \times R_n)$.

By part c, it suffices to find $U(\mathbb{Z}), U(\mathbb{Q})$. It is easy to check that $U(\mathbb{Z}) = \{\ \pm 1\}$ and $U(\mathbb{Q}) = \mathbb{Q} \backslash \{0\}$ under the normal multiplication (as if $a \in \mathbb{Z}$ such that $\exists b \in \mathbb{Z}$ where $a \cdot b = 1$, then $a = \pm 1$ as $b \in \mathbb{Z}$ and the all non-zero elements $q \in \mathbb{Q}$ have inverse $1/q$). Therefore, $U(\mathbb{Z} \times \mathbb{Q}) = \{\pm 1\} \times \mathbb{Q} \backslash \{0\}$. $\square$

## Problem 3

Let $\mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$. We will show this is a ring. Note that $\mathbb{Z}[\sqrt{3}] \subset \mathbb{R}$, and so it suffices to use the subring criterion, as $\mathbb{R}$ is a ring. Note that $0 \in \mathbb{Z}[\sqrt{3}]$, so it is non-empty. Now take $a_1 + b_1\sqrt{3}, a_2 + b_2\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Then $(a_1 + b_1\sqrt{3}) - (a_2 + b_2\sqrt{3}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, as the sum of two integers is an integer. Similarly, $(a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3}) = (a_1a_2 + 3b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Therefore this is a ring. More formally, this proof can also be constructed from the ground up without the subring criterion, checking associativity, distributivity, etc. $\square$

## Problem 4

Take $q := a + b\sqrt{3} \in F \backslash \{0\}$. It suffices to show $q$ has an inverse in $F$. Note that $a, b$ cannot both be zero. Therefore, as $q \neq 0$, $q \in F \subset \mathbb{R}$, we can see that $\frac{1}{a+b\sqrt{3}} = \frac{1}{a+b\sqrt{3}} \cdot \frac{a-b\sqrt{3}}{a-b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2}$. Note that this is valid as $a + b\sqrt{3} \neq 0$, and $0 \neq a - b\sqrt{3}$ because $a, b \in \mathbb{Q}$ and $\sqrt{3} \notin \mathbb{Q}$ (so if $a = b\sqrt{3}$ we have a contradiction). Therefore, as $\mathbb{R}$ is an integral domain (i.e., no zero divisors), $a^2 - 3b^2 \neq 0$. Another way to see this is because if $a^2 - 3b^2 = 0$, then $a^2 = 3b^2 \implies a = \pm\sqrt{3}b \implies \sqrt{3} \in \mathbb{Q}$, a contradiction. In either case, we see that the element $\frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3} = (a + b\sqrt{3})^{-1}$, and as $a, b \in \mathbb{Q}$, so too is $\frac{a}{a^2-3b^2}, \frac{b}{a^2-3b^2} \in \mathbb{Q}$. $\square$

## Problem 5

In this problem we show $U(\mathbb{Z}[x]) = \{\pm 1\} = U(\mathbb{Z})$ (the last equality is done in Problem 2, part d). Take $a \in U(\mathbb{Z}) \subseteq \mathbb{Z}[x]$. Then $\exists b \in \mathbb{Z} \subseteq \mathbb{Z}[x]$ such that $ab = 1 = ba$, and so $a \in U(\mathbb{Z}[x])$, and $\{\pm 1\} \subseteq U(\mathbb{Z}) \subseteq U(\mathbb{Z}[x])$. First note that, given as $\mathbb{Z}$ is an integral domain, there are no zero divisors. Take $p(x) := a_nx^n + \cdots + a_0 \in U(\mathbb{Z}[x])$, where $a_n \neq 0$ (we can do this as zero is not invertible, so there will always be a maximum non-zero coefficient). Then we know $\exists q(x) := b_mx^m + \cdots + b_0 \in U(\mathbb{Z}[x])$ such that $p(x)q(x) = q(x)p(x) = 1$ (and again as with $p(x)$, $b_m \neq 0$). Assume for contradiction that $n > 0$. Then, ignoring the intermediate coefficients for now, we see $a_nb_mx^{n+m} = 0$, and so $a_nb_m = 0$. As $a_n \neq 0 \neq b_m$, and $\mathbb{Z}$ has no zero divisors, we have a contradiction, and therefore, $n = 0$. A similar argument shows $m = 0$. Therefore, $p(x) = a_0, q(x) = b_0$, and $a_0b_0 = 1$. But as $a_0 \in \mathbb{Z}$, this implies $a_0 \in U(\mathbb{Z})$, so $U(\mathbb{Z}) \subseteq U(\mathbb{Z}[x])$.

Now consider $2x+1 \in \mathbb{Z}_8[x]$. We will see $p(x) = 4x^2 + 6x + 1$ is $(2x+1)^{-1}$. As $\mathbb{Z}_8[x]$ is commutative, it suffices to show $(2x+1)p(x) = 1$ (as 1 is the unity of $\mathbb{Z}_8[x]$). We do this by computation– $(2x+1)(4x^2+6x+1) = 8x^3 + (4+12)x^2 + (2+6)x + 1 = 8x^3 + 16x^2 + 8x + 1$, and as $16 \equiv 8 \equiv 0 \mod 8$, $(2x+1)(4x^2+6x+1) = 1$. $\square$

## Problem 6

First note that as $1_A \in A$, $a_0 \cdot 1_A \cdot a_0 = a_0^2 = 1 \in B$, and so $B \neq \emptyset$. Take $b_1, b_2 \in B$. By the subring criterion, it suffices to check $b_1 - b_2, b_1 \cdot b_2 \in B$. We know $b_1 = a_0 b_1' a_0$, $b_2 = a_0 b_2' a_0$, for some $b_1', b_2' \in A$. Now consider $b_1 \cdot b_2 = (a_0 b_1' a_0) \cdot (a_0 b_2' a_0) = a_0(b_1' a_0 a_0 b_2')a_0 = a_0(b_1' b_2')a_0$ as multiplication is associative and $a_0^2 = 1$. As $b_1' b_2' \in A$, we see $b_1 \cdot b_2 \in B$. Now consider $b_1 - b_2 = a_0 b_1' a_0 - a_0 b_2' a_0 = a_0(b_1' a_0 - b_2' a_0) = a_0(b_1' - b_2')a_0 \in B$ as $A$ has distribution and $b_1' - b_2' \in A$. Thus, $B$ is a subring. $\square$ Side note: $a_0^2 = 1 \implies a_0 = a_0^{-1}$, so $B = a_0 A a_0^{-1}$, though note that $A$ isn't a multiplicative group.