Homework #4

Problems to hand in on Thursday, February 14, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) Let m and n be positive integers with $(m, n) = 1$. Show[1] that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Solution. In Problem Set 2, we showed that given $a, b \in \mathbb{Z}$, there is a unique solution modulo mn to the system of equations

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$$

We can rephrase this as saying that there is a well-defined map $\mathbb{Z}_m \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_{mn}$. This map is a ring homomorphism: if

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases} \text{ and } \begin{cases} y \equiv c \mod n \\ y \equiv d \mod m \end{cases}$$

then

$$\begin{cases} xy \equiv ac \mod n \\ xy \equiv bd \mod m \end{cases} \text{ and } \begin{cases} x+y \equiv a+c \mod n \\ x+y \equiv c+d \mod m \end{cases}$$

and this map takes $(1, 1)$ to 1. This map is also surjective. To see that, notice that given $[x]$ in $\mathbb{Z}_{nm}$, we have also shown in Problem Set 2 that the map that sends $[x]_{mn}$ to $[x]_n$ is well-defined, since $n|nm$, and similarly for sending $[x]_{mn}$ to $[x]_m$. That says that given $[x]_{mn} \in \mathbb{Z}_{mn}$, there is a well-defined element $([x]_m, [x]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$, and it is easy to check that the image of $([x]_m, [x]_n)$ under our map is $[x]_{mn}$.

We have a found a surjective ring homomorphism $\mathbb{Z}_m \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_{mn}$. Since these are two rings with mn elements, this ring homomorphism must be injective, and thus an isomorphism.

2) Let V be a vector space. Recall that a function $T : V \to V$ is a *linear transformation* if for all $v, w \in V$ and all $\lambda \in \mathbb{R}$, we have $T(v + w) = T(v) + T(w)$ and $T(\lambda v) = \lambda T(v)$.

(a) Show that the set of linear transformations from V to V, with usual addition, and *composition of functions* as multiplication, forms a ring.

(b) Consider the vector space $\mathbb{R}[x]$ and let $\mathcal{L}(\mathbb{R}[x])$ be the ring of linear transformations of $\mathbb{R}[x]$ as defined in the previous part. Consider the element $\frac{d}{dx} \in \mathcal{L}(\mathbb{R}[x])$. Show that there is an element $F \in \mathcal{L}(\mathbb{R}[x])$ such that $\frac{d}{dx}F = 1_{\mathcal{L}(\mathbb{R}[x])}$, but there is no element $G \in \mathcal{L}(\mathbb{R}[x])$ such that $G\frac{d}{dx} = 1_{\mathcal{L}(\mathbb{R}[x])}$.

Solution.

[1] Hint: You can save a lot of work by referring back to problems from previous homeworks.

(a) We check the axioms. The constant zero function is the zero of this ring; the "identity" function is the one of this ring. Addition is associative: $((f+g)+h)(x) = (f+g)(x) + h(x) = f(x)+g(x)+h(x) = f(x)+(g+h)(x) = (f+(g+h))(x)$, so $(f+g)+h = f+(g+h)$. Commutativity of addition is roughly the same. If f is linear, then $-f$ is linear, so there are additive inverses. Multiplication is associative, because composition of functions is. The distributive laws are the most interesting: $(f(g+h))(x) = f(g(x)+h(x)) = f(g(x)) + f(h(x)) = (fg+fh)(x)$, so $f(g+h) = fg+fh$, and the other distributive law is similar.

(b) Take F to be antidifferentiation (with some choice of constant of integration C). To see no such G exists, note that $\frac{d}{dx}(1) = 0$. We would need to have $G(0) = 1$, but this cannot happen for any linear function.

3) We say a ring R has characteristic n if n is the smallest positive integer such that

$$\underbrace{1 + \cdots + 1}_{\text{n times}} = 0.$$

If no such n exists, we say that R has characteristic 0.

(a) Give examples of a ring of characteristic 0 and a ring of characteristic n for each $n \geqslant 2$.

(b) Suppose that R is a commutative ring of prime characteristic p. Prove that the *Freshman's Dream* holds in R: $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

(c) Suppose that R is a commutative ring of prime characteristic p. Prove that the Frobenius map $r \mapsto r^p$ is a ring homomorphism $R \longrightarrow R$.

(d) Give an example to show that if the characteristic of R is not 2, $r \mapsto r^2$ may not be a ring homomorphism.

Solution.

(a) Easiest example: $\mathbb{Z}$, $\mathbb{Z}_n$.

(b) We use the binomial theorem: $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$. Now, $p | \binom{p}{i}$ for all $1 \leq i \leq n-1$, so these coefficients are zero in R, and the formula then holds.

(c) It takes 1 to 1, rs to $(rs)^p = r^p s^p$, and $r+s$ to $(r+s)^p = r^p + s^p$, using the previous part.

(d) In $\mathbb{Z}$, $(1+1)^2 = 4 \neq 2 = 1^2 + 1^2$.

4) Consider the field $\mathbb{F} = \mathbb{Z}_{13}$. Construct the addition and the multiplication tables for this field and use them to answer the following questions.

(a) Give a reasonable interpretation, in $\mathbb{F}$, for the expressions $2, -4, 3/4, -4/3, \sqrt{-1}$ (and carefully explain your reasoning).

(b) Solve the quadratic equation $x^2 + 6x + 4 = -1$ by *completing the square*. Check your answers!

(c) Now solve the same equation by using the *quadratic formula*. Why is it valid over $\mathbb{F}$? Is it valid over any field?

(d) Use the usual discriminant $D = b^2 - 4ac$ to classify the equations $ax^2 + bx + c = 0$ that have two roots, a single root, or no root in $\mathbb{F}$.

(e) Using the discriminant determine, without solving the equation, the number of roots of the equation $7x^2 + 4x + 3 = 0$.

Solution.

(a) 2 means [2], -4 means $-4 = 9$, $3/4$ would be $3 \cdot 4^{-1} = 9$, and $\sqrt{-1}$ is a number whose square is -1, e.g., 5.

(b) Working in $\mathbb{F}$, we add $(6/2)^2 = 9$ to both sides of the quadratic equation $x^2 + 6x = 7$. We get $x^2 + 6x + 9 = 5$ (again, in $\mathbb{Z}_{11}$). This can be written $(x + 3)^2 = 5$. Now, 5 is a square in two ways in $\mathbb{Z}_{11}$. We have $[4]^2 = [?4]^2 = [7]^2 = 5$. So $(x + 3) = 4$ and $(x + 3) = 7$ both give solutions. The solutions are [1] and [4].

(c) Plugging in the values, and extracting square roots as above, we get the same solutions. The quadratic formula is valid over any field in which $2 = 1+1$ is a unit. The reason is that we derive the formula by completing the square on the equation $ax^2 + bx + c = 0$, which involves only using repeated ring/field axioms. Since we "divide by 2" at some point, we do need to make sure that 2 has a multiplicative inverse.

(d) In $\mathbb{F} = \mathbb{Z}_{11}$, the numbers 0, 1, 4, 9, 5, 3 are the only squares. So $ax^2 + bx + c = 0$ has a solution in $\mathbb{F}$ if and only if $b^2 - 4ac \in \{0, 1, 3, 4, 5, 9\}$. It has two solutions in each case except if $b^2 = 4ac$, where it has exactly one solution.

(e) $b^2 - 4ac = (9)^2 - 4(8)(3) = 4 - 8 = 7$. Since 7 is not a square in $\mathbb{F}$, there are no solutions.