Math 412 Homework 4

Submission Instructions: You are responsible to read these instructions. Failure to submit correctly as described below will result in point deductions or loss of credit for entire problems. Submit these problems on Gradescope by Thursday, February 15th, at 11:59pm. Each problem should be on a separate page (or pages). **You will need to scan a PDF of the assignment AND select the pages belonging to each problem when you submit on gradescope.**

1. (a) If $f : R \to S$ is a homomorphism of rings, show for any $r \in R$ and $n \in \mathbb{Z}$, $f(nr) = nf(r)$.
   (b) Prove that isomorphic rings have the same characteristic.
   (c) If $f : R \to S$ is a homomorphism of rings, must R and S have the same characteristic?

   1. Recall $nr := \underbrace{r + \cdots + r}_{n \text{ times}}$. Therefore $f(nr) = f(\underbrace{r + \cdots + r}_{n \text{ times}}) = \underbrace{f(r) + \cdots + f(r)}_{n \text{ times}} = nf(r)$.
   2. To prove this, we will assume that $f : R \to S$ is an isomorphism. Let m be the characteristic of R, therefore $mr = 0$ for all $r \in R$. Since f is surjective, for all $s \in S$, there exists $r_s \in R$ so that $f(r_s) = s$. By part (a), we have that
   $$0_S = f(0_R) = f(mr_s) = mf(r_s).$$
   Since $s \in S$ is arbitrary, $ms = 0$ for all m. Therefore the characteristic of S is at most m.
   3. No. For example, as we saw in Homework 2, the map
   $$f : \mathbb{Z}_m \to \mathbb{Z}_n$$
   defined by $f([a]_m) = [a]_n$ is well-defined if $n \mid m$. It is also a homomorphism since
   $$f([a]_m + [b]_m) = f([a + b]_m) = [a + b]_n = [a]_n + [b]_n = f([a + b]_n).$$
   But the characteristic of $\mathbb{Z}_m$ is m and the characteristic of $\mathbb{Z}_n$ is n.

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 $G\frac{d}{dx} = 1_{\mathcal{L}(\mathbb{R}[x])}$.

(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. Let d be an integer.

   (a) Prove that $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

   (b) Show that $\mathbb{Z}_7[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}_7\}$ is a field.

   (c) Now assume d is also positive and p is a prime. Determine a necessary and sufficient condition for $\mathbb{Z}_p[\sqrt{d}]$ to be a field.

1. **Solution 1:** We note that $\mathbb{C}$ is a field with regular addition and multiplication. The element $\frac{1}{a^2+b^2}(a-bi)$ is the multiplicative inverse of $a+bi$ for all nonzero elements (the fact that $\mathbb{C}$ is a ring is verified in the book and was verified in class).

   The set $\mathbb{Z}[\sqrt{d}]$ is a subset of $\mathbb{C}$. We show it's a subring. Indeed, $0 = 0 + 0\sqrt{d}$ and $1 = 1 + 0\sqrt{d}$ are both elements of $\mathbb{Z}[\sqrt{d}]$.

   We check that $\mathbb{Z}[\sqrt{d}]$ is closed under subtraction: let $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Z}[d]$. Then $(a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d}) = (a - 1 - a_2) + (b_1 - b_2)\sqrt{d}$. Since $a_1 - a_2 \in \mathbb{Z}$ and $b_1 - b_2 \in \mathbb{Z}$, then $(a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d}) = (a - 1 - a_2) + (b_1 - b_2)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

   We check that $\mathbb{Z}[\sqrt{d}]$ is closed under multiplication: let $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Z}[d]$. Then $(a_1+b_1\sqrt{d})\cdot(a_2+b_2\sqrt{d}) = a_1a_2+b_1b_2d+(a_1b_2+a_2b_1)\sqrt{d}$. Since $a_1a_2+b_1b_2d \in \mathbb{Z}$ and $(a_1b_2 + a_2b_1) \in \mathbb{Z}$, then $(a_1 + b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$.

   Then $\mathbb{Z}[\sqrt{d}]$ is a subring of $\mathbb{C}$, so it is a domain (by an exercise from class).

   Solution 2: First note that if d is a square, then $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}$, which is a domain and we are done. So we may assume d is not a square.

   We first show $\mathbb{Z}[\sqrt{d}]$ is a ring with the usual addition and multiplication.

   - The element $0 = 0 + 0\sqrt{d}$ is the additive identity since $a + 0 = 0 + a = a$ (for all real numbers).
   - The element $1 = 1 + 0\sqrt{d}$ is the multiplicative identity since $1a = a1 = a$ (for all real numbers).

- Addition is associative: let $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d}, a_3 + b_3\sqrt{d} \in \mathbb{Z}[d]$. Then

$$\begin{aligned} a_1 + b_1\sqrt{d} + (a_2 + b_2\sqrt{d} + a_3 + b_3\sqrt{d}) &= a_1 + b_1\sqrt{d} + ((a_2 + a_3) + (b_2 + b_3)\sqrt{d}) \\ &= ((a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{d}) \\ &= ((a_1 + a_2) + (b_1 + b_2)\sqrt{d} + a_3 + b_3\sqrt{d} \\ &= ((a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d})) + a_3 + b_3\sqrt{d} \end{aligned}$$

- Addition is commutative: let $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Z}[d]$. Then

$$\begin{aligned} (a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) &= (a_1 + a_2) + (b_1 + b_2)\sqrt{d} \\ &= (a_2 + a_1) + (b_2 + b_1)\sqrt{d} \\ &= (a_2 + b_2\sqrt{d}) + (a_1 + b_1\sqrt{d}) \end{aligned}$$

  Let $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Z}[d]$. Now assume that $(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = 0$. By distributivity, we have

$$\begin{aligned} 0 &= (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) \\ &= a_1a_2 + a_2b_1\sqrt{d} + a_1b_2\sqrt{d} + b_1b_2d \\ &= (a_1a_2 + b_1b_2d) + (a_2b_1 + a_1b_2)\sqrt{d}. \end{aligned}$$

- Multiplication is associative: let $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d}, a_3 + b_3\sqrt{d} \in \mathbb{Z}[d]$. Then

$$\begin{aligned} &(a_1 + b_1\sqrt{d}) \times ((a_2 + b_2\sqrt{d}) \times (a_3 + b_3\sqrt{d})) = (a_1 + b_1\sqrt{d}) \times ((a_2a_3 + b_2b_3) + (a_2b_3 + b_2a_3)\sqrt{d}) \\ &= ((a_1a_2a_3 + a_1b_2b_3 + b_1a_2b_3d + b_1b_2a_3d) + (a_1a_2a_3 + a_1b_2b_3 + b_1a_2a_3 + b_1b_2b_3)\sqrt{d}) \\ &= ((a_1a_2 + b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{d}) \times (a_3 + b_3\sqrt{d}) \\ &= ((a_1 + b_1\sqrt{d}) \times (a_2 + b_2\sqrt{d})) \times (a_3 + b_3\sqrt{d}) \end{aligned}$$

  Where we used commutativity of addition to go from the first to second and second to third lines. We also used the distributivity of real numbers to reduce the number of steps.
- Multiplication is commutative (note this is not required to prove that $\mathbb{Z}[d]$ is a ring, but it is true and will help in the proof of distributivity): let $a_1+b_1\sqrt{d}, a_2+b_2\sqrt{d} \in \mathbb{Z}[d]$. Then

$$\begin{aligned} (a_1 + b_1\sqrt{d}) \times (a_2 + b_2\sqrt{d}) &= (a_1a_2 + b_1b_2d) + (b_1a_2 + a_1b_2)\sqrt{d} \\ &= (a_2a_1 + b_2b_1d) + (a_2b_1 + b_2a_1)\sqrt{d} \\ &= (a_2 + b_2\sqrt{d}) \times (a_1 + b_1\sqrt{d}) \end{aligned}$$

- Distributivity follows similarly.

Now assume that $0 = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})$ Then it is also true that

$$0 = (a_1 + b_1\sqrt{d})(a_1 - b_1\sqrt{d})(a_2 + b_2\sqrt{d})(a_2 - b_2\sqrt{d}) = (a_1^2 - b_1^2d)(a_2^2 - b_2^2d).$$

(drawing inspiration from the inverse in $\mathbb{C}$)

Since $a_1^2 - b_1^2 d$ and $a_2^2 - b_2^2 d$ are both integers. Since $\mathbb{Z}$ is a domain, one of $a_1^2 - b_1^2 d$ and $a_2^2 - b_2^2 d$ must be 0. But this implies $a_1^2 = b_1^2 d$ or $a_2^2 = b_2^2 d$. Without loss of generality, assume $a_1^2 = b_1^2 d$.

We have two cases:

either $a_1 = b_1 = 0$ and we are done or

he integer b_1^2 divides a_1^2, we can write $d = \frac{a_1^2}{b_1^2} = \left(\frac{a_1}{b_1}\right)^2$. Because we assumed (a very long time ago) that d was not a square, this is a contradiction.

Therefore $a_1 = b_1 = 0$ and $\mathbb{Z}[\sqrt{d}]$ is a domain.

2. Using reasoning similar to that in solution 2 of part a), we can prove that $\mathbb{Z}_7[\sqrt{d}]$ is a ring. To see it's a field, we need only find the inverse for all nonzero elements. We know that $\mathbb{Z}_7$ is a field, so all nonzero elements have inverses.

   Inspired by how we find inverses in $\mathbb{C}$, when a and b are not both 0, we have that the inverse of $a + b\sqrt{3}$ should be $(a - b\sqrt{3})(a^2 - 3b^2)^{-1}$ (where we know $(a^2 - 3b^2)^{-1}$ exists because $\mathbb{Z}_7$ is a field).

   We check that we are right:

$$(a + b\sqrt{3})(a - b\sqrt{3})(a^2 - 3b^2)^{-1} = (a^2 - 9b^2)(a^2 - 3b^2)^{-1} = 1.$$

3. It must be that d is not a perfect square. We repeat the argument in b) replacing 7 with p and 3 with d. We use the assumption that d is not a multiple of p in the step where we find the inverse of $a + b\sqrt{d}$. Indeed, we require that $(a^2 - db^2)$ is nonzero (hence invertible) in $\mathbb{Z}_p$. The element $(a^2 - db^2)$ is zero in $\mathbb{Z}_p$ if and only if p divides $a^2 - db^2$.

4. Let R be a commutative ring in which $a^2 = 0$ only if $a = 0$. Show that if $q(x) \in R[x]$ is a zero divisor in $R[x]$, then if:

$$q(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n,$$

there is an element $b \neq 0$ in R such that $ba_0 = ba_1 = \cdots = ba_n = 0$.

First, we will use the fact that if $q(x)$ is a zero divisor with $g(x)q(x)$, then for any $c \in R$, $cq(x)$ is a zero divisor with $g(x)q(x)$.

We claim that the desired coefficient b is a power of the leading coefficient of $g(x)$. We'll use induction on the degree of $q(x)$, but the proof will be structured more like a recursive argument.

For the base case we let the degree of $q(x)$ be 0. Then $q(x) = a_0$.Then any $g(x)$ so that $0 = g(x)q(x) = g(x)a_0$ must have the property that all coefficients of $g(x)$ times a_0 are zero. In particular, if b is the leading coefficient of $g(x)$, it must be true that $0 = bq(x) = ba_0$. So the statement is true.

Let $g(x)$ be a polynomial such that $q(x)g(x) = 0$. Let $g(x) = b_0 x^m + b_1 x^m + \cdots + b_m$. The only term of $q(x)g(x)$ of degree $m + n$ has coefficient $a_0 b_0$. Since $q(x)g(x) = 0$, it must be true that $a_0 b_0 = 0$.

Then

$$b_0 q(x) = 0 + b_0 a_1 x^n + b_0 a_2 x^{n-2} + \cdots b_0 a_n$$

is also a zero divisor, call it $q_1(x)$. The degree of $q_1(x)$ is strictly less than the degree of $q(x)$ (it could be even be less than $n-1$ if more than just the first term cancels), call this degree k. In fact:

$$0 = g(x)(b_0 q(x)) = b_0 g(x)(q(x))$$

(since the ring is commutative). Let $q_1(x) = b_0 q(x) = b_0 a_{n-k} x^k + \cdots b_0 a_n$. Since $g(x)q_1(x) = 0$, it follows by the same argument as above that $b_0(b_0 a_{n-k}) = 0$. Let $b_1 = b_0^2$ and repeat the process with $q_2(x) = b_1 q(x) = b_0 q_1(x)$. Continue this process recursively by defining $b_i = b_{i-1}^2$ and $q_{i+1}(x) = b_i q(x)$. Repeat until $q_\ell(x) = b_0^{2^{\ell-1}} q(x) = 0$ for some ℓ.

It remains to show that $b \neq 0$. In our construction we had that $b_0 \neq 0$ and therefore by assumption $b_1 = b_0^2 \neq 0$. Since we constructed each $b_i = b_{i-1}^2$, we have that $b_i = 0$ if and only if $b_{i-1} = 0$ if and only if $b_0 = 0$. Since b_0 was the leading coefficient of $g(x)$, we can assume that it is nonzero and we are done.

Note: A proof starting at the constant term and going up would also work, but the fact that the leading coefficient is named a_0 makes it easier to start with the highest power first.