University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Homework 4

Darij Grinberg

May 15, 2019

due date: **Wednesday, 13 March 2019** at the beginning of class, or before that by email or canvas.
Please solve **at most 3 of the 6 exercises**!

1 Exercise 1: Equivalence relations always come from maps

1.1 Problem

Let S be a set.

Recall that if T is a further set, and if $f : S \to T$ is a map, then $\underset{f}{\equiv}$ denotes the relation on S defined by

$$\left(a \underset{f}{\equiv} b\right) \iff (f(a) = f(b)).$$

This is an equivalence relation, called "equality upon applying f" or "equality under f".

Now, let $\sim$ be **any** equivalence relation on S. Prove that $\sim$ has the form $\underset{f}{\equiv}$ for a properly chosen set T and a properly chosen $f : S \to T$.

More precisely, prove that $\sim$ equals $\underset{f}{\equiv}$, where T is the quotient set $S/\sim$ and where $f : S \to T$ is the projection map $\pi_\sim : S \to S/\sim$.

[**Hint:** To prove that two relations R_1 and R_2 on S are equal, you need to check that every pair (a, b) of elements of S satisfies the equivalence $(aR_1b) \iff (aR_2b)$.]

1.2 Solution

[...]

---

2 Exercise 2: Totient-related sum

2.1 Problem

Let $n > 1$ be an integer. Prove that

$$\sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i \perp n}} i = n\phi(n)/2.$$

2.2 Solution

[...]

---

3 Exercise 3: Dual numbers

3.1 Problem

Recall that complex numbers were defined as pairs (a, b) of real numbers, with entrywise addition and subtraction and a certain weird-looking multiplication.

Let me define a different kind of "numbers": the *dual numbers.* (The word "numbers" may appear a bit inappropriate for them, but it is not exactly a trademark...)

We define a *dual number* to be a pair (a, b) of two real numbers a and b.

We let $\mathbb{D}$ be the set of all dual numbers.

For each real number r, we denote the dual number $(r, 0)$ by $r_{\mathbb{D}}$.

We let ε denote the dual number $(0, 1)$.

Define three binary operations $+$, $-$ and $\cdot$ on $\mathbb{D}$ by setting

$$(a, b) + (c, d) = (a + c, b + d), \qquad (1)$$
$$(a, b) - (c, d) = (a - c, b - d), \qquad (2)$$
$$(a, b) \cdot (c, d) = (ac, ad + bc) \qquad (3)$$

for all $(a, b) \in \mathbb{D}$ and $(c, d) \in \mathbb{D}$.

(Note that the only difference to complex numbers is the definition of $\cdot$, which is lacking a $-bd$ term.)

Again, we are following standard PEMDAS rules[1] for the order of operations, and we abbreviate $\alpha \cdot \beta$ as $\alpha\beta$.

(a) Prove that $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{D}$.

[1] `https://en.wikipedia.org/wiki/Order_of_operations`

You can use the following properties of dual numbers without proof (they are all essentially obvious):

- We have $\alpha + \beta = \beta + \alpha$ for any $\alpha, \beta \in \mathbb{D}$.
- We have $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{D}$.
- We have $\alpha + 0_{\mathbb{D}} = 0_{\mathbb{D}} + \alpha == \alpha$ for any $\alpha \in \mathbb{D}$.
- We have $\alpha \cdot 1_{\mathbb{D}} = 1_{\mathbb{D}} \cdot \alpha = \alpha$ for any $\alpha \in \mathbb{D}$.
- We have $\alpha \cdot \beta = \beta \cdot \alpha$ for any $\alpha, \beta \in \mathbb{D}$.
- We have $\alpha \cdot (\beta + \gamma) = \alpha\beta + \alpha\gamma$ and $(\alpha + \beta) \cdot \gamma = \alpha\gamma + \beta\gamma$ for any $\alpha, \beta, \gamma \in \mathbb{D}$.
- We have $\alpha \cdot 0_{\mathbb{D}} = 0_{\mathbb{D}} \cdot \alpha = 0_{\mathbb{D}}$ for any $\alpha \in \mathbb{D}$.
- If $\alpha, \beta, \gamma \in \mathbb{D}$, then we have the equivalence $(\alpha - \beta = \gamma) \iff (\alpha = \beta + \gamma)$.

We shall identify each real number r with the dual number $r_{\mathbb{D}} = (r, 0)$.

(b) Prove that $a + b\varepsilon = (a, b)$ for any $a, b \in \mathbb{R}$.

An *inverse* of a dual number $\alpha \in \mathbb{D}$ means a dual number β such that $\alpha\beta = 1_{\mathbb{D}}$. This inverse is unique, and is called α^{-1}.

(c) Prove that a dual number $\alpha = a + b\varepsilon$ (with $a, b \in \mathbb{R}$) has an inverse if and only if $a \neq 0$.

(d) If $a, b \in \mathbb{R}$ satisfy $a \neq 0$, prove that the inverse of the dual number $a + b\varepsilon$ is $\dfrac{1}{a} - \dfrac{b}{a^2}\varepsilon$.

We define finite sums and products of dual numbers in the usual way (i.e., just as finite sums and products of real numbers were defined). Here, an empty sum of dual numbers is always understood to be $0_{\mathbb{D}}$, whereas an empty product of dual numbers is always understood to be $1_{\mathbb{D}}$.

If α is a dual number and $k \in \mathbb{N}$, then the *k-th power of α* is defined to be the dual number $\underbrace{\alpha\alpha\cdots\alpha}_{k \text{ factors}}$. This k-th power is denoted by α^k. Thus, in particular, $\alpha^0 = \underbrace{\alpha\alpha\cdots\alpha}_{0 \text{ factors}} =$ (empty product) $= 1_{\mathbb{D}}$.

(e) Let $P(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$ be a polynomial with real coefficients. Prove that

$$P(a + b\varepsilon) = P(a) + bP'(a)\,\varepsilon \qquad \text{for any } a, b \in \mathbb{R}.$$

Here, P' denotes the derivative of P, which is defined by

$$P'(x) = ka_k x^{k-1} + (k-1)\,a_{k-1}x^{k-2} + \cdots + 1a_1 x^0.$$

3.2 Remark

The dual number ε is one of the simplest "rigorous infinitesimals" that appear in mathematics. Part **(e)** of the exercise shows that we can literally write $P(a+\varepsilon) = P(a) + P'(a)\varepsilon$ when P is a polynomial, without having to compute any limits. It is tempting to "solve" this equation for $P'(a)$, thus obtaining something like $P'(a) = \dfrac{P(a+\varepsilon) - P(a)}{\varepsilon}$. However, this needs to be taken with a grain of salt, since ε has no inverse and the fraction $\dfrac{P(a+\varepsilon) - P(a)}{\varepsilon}$ is not uniquely determined. There are other, subtler ways to put infinitesimals on a firm algebraic footing, but dual numbers are already useful in some situations.

Note that dual numbers have *zero-divisors*: i.e., there exist nonzero dual numbers a and b such that $ab = 0$. The simplest example is probably $\varepsilon^2 = 0$ (despite $\varepsilon \neq 0$).

3.3 Solution

[...]

4 Exercise 4: $\mathbb{Z}\left[\sqrt{2}\right]$

4.1 Problem

Let $\mathbb{Z}\left[\sqrt{2}\right]$ denote the set of all reals of the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. We shall call such reals $\sqrt{2}$*-integers.*

(a) Prove that any $\alpha, \beta \in \mathbb{Z}\left[\sqrt{2}\right]$ satisfy $\alpha + \beta \in \mathbb{Z}\left[\sqrt{2}\right]$ and $\alpha - \beta \in \mathbb{Z}\left[\sqrt{2}\right]$ and $\alpha\beta \in \mathbb{Z}\left[\sqrt{2}\right]$.

(b) Prove that every element of $\mathbb{Z}\left[\sqrt{2}\right]$ can be written as $a + b\sqrt{2}$ for a **unique** pair (a, b) of integers. (In other words, if four integers a, b, c, d satisfy $a + b\sqrt{2} = c + d\sqrt{2}$, then $a = c$ and $b = d$.)

For any $\alpha \in \mathbb{Z}\left[\sqrt{2}\right]$, define the $\sqrt{2}$*-norm* $N_2(\alpha)$ of α by $N_2(\alpha) = a^2 - 2b^2$, where α is written in the form $\alpha = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. This is well-defined by part **(b)** of this exercise.

(c) Prove that $N_2(\alpha\beta) = N_2(\alpha) N_2(\beta)$ for all $\alpha, \beta \in \mathbb{Z}\left[\sqrt{2}\right]$.

Let $(p_0, p_1, p_2, \ldots)$ be the sequence of nonnegative integers defined recursively by

$$p_0 = 0, \qquad p_1 = 1, \qquad \text{and} \qquad p_n = 2p_{n-1} + p_{n-2} \text{ for all } n \geq 2.$$

(Thus, $p_2 = 2$ and $p_3 = 5$ and $p_4 = 12$ and so on.)

(d) Prove that $p_{n+1}p_{n-1} - p_n^2 = (-1)^n$ for each $n \geq 1$.

(e) Prove that $\left(p_{n-1} + p_n + p_n\sqrt{2}\right) \cdot \left(p_{n-1} + p_n - p_n\sqrt{2}\right) = (-1)^n$ for each $n \geq 1$.

[**Hint:** For **(d)**, use induction.]

4.2 Remark

The set $\mathbb{Z}\left[\sqrt{2}\right]$ of $\sqrt{2}$-integers is rather similar to the set $\mathbb{Z}[i]$ of Gaussian integers: the former has elements of the form $a+b\sqrt{2}$ with $a,b\in\mathbb{Z}$, while the latter has elements of the form $a+b\sqrt{-1}$ with $a,b\in\mathbb{Z}$. The $\sqrt{2}$-norm on $\mathbb{Z}\left[\sqrt{2}\right]$ is an analogue of the (usual) norm on $\mathbb{Z}[i]$. However, visually speaking, the latter set is "spread out" in the Euclidean plane, while the former is "concentrated" on the real line (and actually everywhere dense on it – i.e., every little interval on the real line has a $\sqrt{2}$-integer inside it). The difference has algebraic consequences; in particular, there are only four units $(1,-1,i,-i)$ in $\mathbb{Z}[i]$, whereas $\mathbb{Z}\left[\sqrt{2}\right]$ has infinitely many units (namely, part **(e)** of the exercise shows that $p_{n-1}+p_n+p_n\sqrt{2}$ is a unit for each $n\geq 1$).

4.3 Solution

[...]

---

5 Exercise 5: Euler's theorem for non-coprime integers

5.1 Problem

Let a be an integer, and let n be a positive integer. Prove that $a^n\equiv a^{n-\phi(n)} \mod n$.

5.2 Solution

[...]

---

6 Exercise 6: Wilson strikes again

6.1 Problem

Let p be an odd prime. Write p in the form $p=2k+1$ for some $k\in\mathbb{N}$. Prove that $k!^2\equiv-(-1)^k \mod p$.

[**Hint:** Each $j\in\mathbb{Z}$ satisfies $j(p-j)\equiv -j^2 \mod p$.]

6.2 Solution

[...]

References

[Grinbe19] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.

http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see https://github.com/darijgr/detnotes/releases/tag/2019-01-10 .