University of Minnesota, School of Mathematics

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

Darij Grinberg

May 19, 2019

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

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

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

See the class notes, where this is Exercise 3.3.3. (The numbering may shift; it is one of the exercises in the "Equivalence classes" section.)

---

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

See the class notes, where this is Exercise 2.14.5. (The numbering may shift; it is one of the exercises in the "Euler's totient function (ϕ-function)" section.)

---

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

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

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 $\alpha\beta$.

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

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

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 $\alpha + 0_{\mathbb{D}} = 0_{\mathbb{D}} + \alpha$ 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, $\alpha^0 = \underbrace{\alpha\alpha\cdots\alpha}_{0 \text{ factors}} = (\text{empty product}) = 1_{\mathbb{D}}$.

(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

(a) Let $\alpha, \beta, \gamma \in \mathbb{D}$. We must prove that $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.

We have $\alpha \in \mathbb{D}$; in other words, α is a dual number. Thus, α is a pair (a, b) of two real numbers a and b. Consider these a and b.

We have $\beta \in \mathbb{D}$; in other words, β is a dual number. Thus, β is a pair (c, d) of two real numbers c and d. Consider these c and d.

We have $\gamma \in \mathbb{D}$; in other words, γ is a dual number. Thus, γ is a pair (e, f) of two real numbers e and f. Consider these e and f.

Comparing the equalities

$$\underbrace{\alpha}_{=(a,b)} \cdot \left(\underbrace{\beta}_{=(c,d)} \cdot \underbrace{\gamma}_{=(e,f)} \right) = (a,b) \cdot \underbrace{((c,d)\cdot(e,f))}_{\substack{=(ce,cf+de) \\ \text{(by the definition of} \\ \text{the operation } \cdot \text{ on } \mathbb{D})}} = (a,b)\cdot(ce, cf+de)$$

$$= \left(\underbrace{a\,(ce)}_{=ace}, \underbrace{a\,(cf+de) + b\,(ce)}_{=acf+ade+bce} \right)$$

(by the definition of the operation $\cdot$ on $\mathbb{D}$)

$$= (ace, acf + ade + bce)$$

and

$$\left(\underbrace{\alpha}_{=(a,b)} \cdot \underbrace{\beta}_{=(c,d)} \right) \cdot \underbrace{\gamma}_{=(e,f)} = \underbrace{((a,b)\cdot(c,d))}_{\substack{=(ac,ad+bc) \\ \text{(by the definition of} \\ \text{the operation } \cdot \text{ on } \mathbb{D})}} \cdot (e,f) = (ac, ad+bc)\cdot(e,f)$$

$$= \left(\underbrace{(ac)\,e}_{=ace}, \underbrace{(ac)\,f + (ad+bc)\,e}_{=acf+ade+bce} \right)$$

(by the definition of the operation $\cdot$ on $\mathbb{D}$)

$$= (ace, acf + ade + bce),$$

we obtain $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$. This solves part **(a)** of the exercise.

(b) Let $a, b \in \mathbb{R}$. Then, the definition of $a_{\mathbb{D}}$ yields $a_{\mathbb{D}} = (a, 0)$, whereas the definition of $b_{\mathbb{D}}$ yields $b_{\mathbb{D}} = (b, 0)$. The definition of ε yields $\varepsilon = (0, 1)$. Thus,

$$\underbrace{a_{\mathbb{D}}}_{=(a,0)} + \underbrace{b_{\mathbb{D}}}_{=(b,0)} \underbrace{\varepsilon}_{=(0,1)} = (a,0) + \underbrace{(b,0)\cdot(0,1)}_{\substack{=(b\cdot 0, b\cdot 1+0\cdot 0) \\ \text{(by the definition of} \\ \text{the operation } \cdot \text{ on } \mathbb{D})}} = (a,0) + \left(\underbrace{b\cdot 0}_{=0}, \underbrace{b\cdot 1 + 0\cdot 0}_{=b} \right)$$

$$= (a,0) + (0,b) = \left(\underbrace{a+0}_{=a}, \underbrace{0+b}_{=b} \right) \qquad \left(\begin{array}{c} \text{by the definition of} \\ \text{the operation } + \text{ on } \mathbb{D} \end{array} \right)$$

$$= (a, b)\,.$$

Since we identify the real numbers a and b with the dual numbers $a_{\mathbb{D}}$ and $b_{\mathbb{D}}$, we can rewrite this equality as $a + b\varepsilon = (a, b)$. This solves part **(b)** of the exercise.

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

In other words, we must prove the logical equivalence

$$(\alpha \text{ has an inverse}) \iff (a \neq 0)\,. \tag{4}$$

We shall prove the "$\Longleftarrow$" and "$\Longrightarrow$" parts of this equivalence separately:

[*Proof of the "$\Longleftarrow$" direction of (4):* Assume that $a \neq 0$. We must prove that α has an inverse.

The real numbers $\dfrac{1}{a}$ and $\dfrac{b}{a^2}$ are well-defined (since $a \neq 0$). Hence, the dual number $\left(\dfrac{1}{a}, -\dfrac{b}{a^2} \right)$ is well-defined.

Part **(b)** of this exercise yields $a + b\varepsilon = (a, b)$. Hence, $\alpha = a + b\varepsilon = (a, b)$. Thus,

$$\underbrace{\alpha}_{=(a,b)} \cdot \left(\frac{1}{a}, -\frac{b}{a^2} \right) = (a,b) \cdot \left(\frac{1}{a}, -\frac{b}{a^2} \right) = \left(\underbrace{a\cdot\frac{1}{a}}_{=1}, \underbrace{a\cdot\left(-\frac{b}{a^2}\right) + b\cdot\frac{1}{a}}_{=0} \right)$$

$$\text{(by the definition of the operation } \cdot \text{ on } \mathbb{D})$$

$$= (1,0) = 1_{\mathbb{D}} \qquad \text{(since the definition of } 1_{\mathbb{D}} \text{ yields } 1_{\mathbb{D}} = (1,0))\,.$$

In other words, the dual number $\left(\dfrac{1}{a}, -\dfrac{b}{a^2} \right)$ is an inverse of α (by the definition of "inverse"). Hence, the dual number α has an inverse (namely, $\left(\dfrac{1}{a}, -\dfrac{b}{a^2} \right)$). This proves the "$\Longleftarrow$" direction of (4).]

[*Proof of the "$\Longrightarrow$" direction of (4):* Assume that α has an inverse. We must prove that $a \neq 0$.

We have assumed that α has an inverse. Let β be such an inverse. Thus, β is an inverse of α. In other words, β is a dual number such that $\alpha\beta = 1_{\mathbb{D}}$ (by the definition of "inverse").

Part **(b)** of this exercise yields $a + b\varepsilon = (a, b)$. Hence, $\alpha = a + b\varepsilon = (a, b)$.

But β is a dual number. Thus, β is a pair (c, d) of two real numbers c and d. Consider these c and d.

We have $\alpha\beta = 1_{\mathbb{D}} = (1,0)$ (by the definition of $1_{\mathbb{D}}$). Thus,

$$(1,0) = \underbrace{\alpha}_{=(a,b)}\underbrace{\beta}_{=(c,d)} = (a,b)\cdot(c,d) = (ac, ad+bc) \qquad \left(\begin{array}{c}\text{by the definition of the}\\ \text{operation } \cdot \text{ on } \mathbb{D}\end{array}\right).$$

Thus, $1 = ac$ and $0 = ad+bc$. From $1 = ac$, we conclude that $ac = 1 \neq 0$ and therefore $a \neq 0$. This proves the "$\Longrightarrow$" direction of (4).]

We thus have proven both directions of the equivalence (4). Thus, (4) is proven, and part **(c)** of the exercise is solved.

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

The real numbers $\dfrac{1}{a}$ and $\dfrac{b}{a^2}$ are well-defined (since $a \neq 0$). Hence, the dual number $\left(\dfrac{1}{a}, -\dfrac{b}{a^2}\right)$ is well-defined. Part **(b)** of this exercise (applied to $\dfrac{1}{a}$ and $-\dfrac{b}{a^2}$ instead of a and b) yields $\dfrac{1}{a} + \left(-\dfrac{b}{a^2}\right)\varepsilon = \left(\dfrac{1}{a}, -\dfrac{b}{a^2}\right)$.

Part **(b)** of this exercise yields $a + b\varepsilon = (a,b)$. Hence,

$$\begin{aligned}
&\underbrace{(a+b\varepsilon)}_{=(a,b)}\cdot \underbrace{\left(\frac{1}{a} - \frac{b}{a^2}\varepsilon\right)}_{=\frac{1}{a}+\left(-\frac{b}{a^2}\right)\varepsilon=\left(\frac{1}{a},-\frac{b}{a^2}\right)} \\
&= (a,b)\cdot\left(\frac{1}{a}, -\frac{b}{a^2}\right) = \left(\underbrace{a\cdot\frac{1}{a}}_{=1}, \underbrace{a\cdot\left(-\frac{b}{a^2}\right) + b\cdot\frac{1}{a}}_{=0}\right) \\
&\qquad \text{(by the definition of the operation } \cdot \text{ on } \mathbb{D}) \\
&= (1,0) = 1_{\mathbb{D}} \qquad \left(\text{since the definition of } 1_{\mathbb{D}} \text{ yields } 1_{\mathbb{D}} = (1,0)\right).
\end{aligned}$$

In other words, the dual number $\dfrac{1}{a} - \dfrac{b}{a^2}\varepsilon$ is an inverse of $a+b\varepsilon$ (by the definition of "inverse"). Hence, the dual number $a+b\varepsilon$ has a unique inverse (because any dual number that has an inverse must have a unique inverse), and this inverse is $\dfrac{1}{a} - \dfrac{b}{a^2}\varepsilon$. This solves part **(d)** of the exercise.

(e) We will use two auxiliary claims:

Claim 1: Let J be a finite set. For each $j \in J$, let a_j and b_j be two real numbers. Then,

$$\sum_{j\in J}(a_j, b_j) = \left(\sum_{j\in J} a_j, \sum_{j\in J} b_j\right)$$

(as dual numbers). (Here, the "$\sum\limits_{j\in J}$" sign on the left hand side stands for a sum of finitely many dual numbers; this is defined just as we defined sums of finitely

many integers or real numbers or complex numbers.[2])

[*Proof of Claim 1:* This claim can be proven by a straightforward induction on $|J|$, using the definition of the operation $+$ on $\mathbb{D}$. (We leave the details to the reader.)]

Claim 2: Let $a, b \in \mathbb{R}$. Then, in $\mathbb{D}$, we have

$$(a,b)^k = \left(a^k, ka^{k-1}b\right) \qquad \text{for every } k \in \mathbb{N}.$$

(Here, we agree to understand the expression "ka^{k-1}" to mean 0 when $k = 0$, even if its sub-expression "a^{k-1}" may be meaningless[3].)

[*First proof of Claim 2:* We shall prove Claim 2 by induction on k:

Induction base: We have $(a,b)^0 = 1_{\mathbb{D}} = (1,0)$ (by the definition of $1_{\mathbb{D}}$). Comparing this with $\left(\underbrace{a^0}_{=1}, \underbrace{0a^{0-1}b}_{=0}\right) = (1,0)$, we obtain $(a,b)^0 = (a^0, 0a^{0-1}b)$. In other words, Claim 2 holds for $k = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that Claim 2 holds for $k = m$. We must prove that Claim 2 holds for $k = m+1$.

We have assumed that Claim 2 holds for $k = m$. In other words, we have $(a,b)^m = (a^m, ma^{m-1}b)$. Now,

$$(a,b)^{m+1} = (a,b) \cdot \underbrace{(a,b)^m}_{=(a^m, ma^{m-1}b)} = (a,b) \cdot \left(a^m, ma^{m-1}b\right) = \left(aa^m, ama^{m-1}b + ba^m\right)$$

(by the definition of the operation $\cdot$ on $\mathbb{D}$). But we have $ama^{m-1}b = m\underbrace{aa^{m-1}}_{=a^m}b = ma^m b$. (Strictly speaking, this computation is only justified when $m \neq 0$, because we agreed to give the expression "ka^{k-1}" special treatment when $k = 0$. But it is clear that the equality $ama^{m-1}b = ma^m b$ also holds when $m = 0$.) Thus,

$$(a,b)^{m+1} = \left(\underbrace{aa^m}_{=a^{m+1}}, \underbrace{ama^{m-1}b}_{=ma^m b} + \underbrace{ba^m}_{=a^m b}\right) = \left(a^{m+1}, \underbrace{ma^m b + a^m b}_{=(m+1)a^m b}\right)$$

$$= \left(a^{m+1}, (m+1) \underbrace{a^m}_{\substack{=a^{(m+1)-1} \\ (\text{since } m=(m+1)-1)}} b\right) = \left(a^{m+1}, (m+1)\, a^{(m+1)-1}b\right).$$

In other words, Claim 2 holds for $k = m+1$. This completes the induction step. Thus, Claim 2 is proven by induction.]

The proof we just gave for Claim 2 was straightforward and completely elementary; for the sake of instructivity, let us next outline a different proof of Claim 2, which relies on the binomial formula. First, we recall that the binomial formula (see, e.g., Theorem 2.17.13 in the class notes) says that any real numbers x and y and any $n \in \mathbb{N}$ satisfy

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{5}$$

[2] Recall that empty sums of dual numbers are defined to be $0_{\mathbb{D}} = (0,0)$.

[3] The sub-expression "a^{k-1}" is indeed meaningless when $a = 0$ and $k = 0$.

We can replace "real numbers" by "dual numbers" in this statement (i.e., we can let x and y be dual numbers instead of being real numbers) without sacrificing its correctness; indeed, the very same argument that proves (5) for arbitrary real numbers x and y (by induction on n) will also prove (5) for dual numbers x and y. This is because the basic rules of addition, multiplication and taking powers that hold for real numbers all hold for dual numbers as well[4]. So we know that (5) holds whenever x and y are dual numbers. In other words, any dual numbers x and y and any $n \in \mathbb{N}$ satisfy

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m} \tag{6}$$

(here, we have renamed the summation index k as m).

Let us also observe that $\varepsilon^2 = 0$. (Indeed,

$$\begin{aligned}
\varepsilon^2 &= \underbrace{\varepsilon}_{=(0,1)} \cdot \underbrace{\varepsilon}_{=(0,1)} = (0,1)\cdot(0,1) = \Big(\underbrace{0\cdot 0}_{=0}, \underbrace{0\cdot 1 + 1\cdot 0}_{=0}\Big) \\
&\qquad \text{(by the definition of the operation } \cdot \text{ on } \mathbb{D}) \\
&= (0,0) = 0.
\end{aligned}$$

)

We are now ready to give our second proof of Claim 2:

[*Second proof of Claim 2 (sketched):* It is easy to see that Claim 2 holds for $k = 0$. Thus, for the rest of this proof, we WLOG assume that $k \neq 0$. Hence, $k \geq 1$ (since $k \in \mathbb{N}$).

Part **(b)** of this exercise yields $a + b\varepsilon = (a, b)$. Hence, $(a, b) = a + b\varepsilon$. Thus,

$$\begin{aligned}
(a,b)^k &= (a+b\varepsilon)^k = \sum_{m=0}^{k} \binom{k}{m} a^m (b\varepsilon)^{k-m} \\
&\qquad \text{(by (6), applied to } x = a \text{ and } y = b\varepsilon \text{ and } n = k) \\
&= \sum_{m=0}^{k-2} \binom{k}{m} a^m \underbrace{(b\varepsilon)^{k-m}}_{=b^{k-m}\varepsilon^{k-m}} + \underbrace{\binom{k}{k-1}}_{\substack{=k \\ \text{(this is easy} \\ \text{to check)}}} a^{k-1} \underbrace{(b\varepsilon)^{k-(k-1)}}_{=(b\varepsilon)^1 = b\varepsilon} + \underbrace{\binom{k}{k}}_{\substack{=1 \\ \text{(this is easy} \\ \text{to check)}}} a^k \underbrace{(b\varepsilon)^{k-k}}_{=(b\varepsilon)^0=1} \\
&\qquad \left(\begin{array}{c} \text{here, we have split off the addends for } m = k-1 \\ \text{and for } m = k \text{ from the sum (which is allowed,} \\ \text{because } k \geq 1 \text{ shows that both of these addends exist)} \end{array} \right) \\
&= \sum_{m=0}^{k-2} \binom{k}{m} a^m b^{k-m} \underbrace{\varepsilon^{k-m}}_{\substack{=\varepsilon^2\varepsilon^{(k-m)-2} \\ \text{(since } k-m\geq 2 \\ \text{(because } m\leq k-2))}} + k a^{k-1} b\varepsilon + a^k \\
&= \sum_{m=0}^{k-2} \binom{k}{m} a^m b^{k-m} \underbrace{\varepsilon^2}_{=0} \varepsilon^{(k-m)-2} + k a^{k-1} b\varepsilon + a^k = k a^{k-1} b\varepsilon + a^k \\
&= a^k + k a^{k-1} b\varepsilon = \left(a^k, k a^{k-1} b\right)
\end{aligned}$$

(by part **(b)** of the exercise, applied to a^k and $ka^{k-1}b$ instead of a and b). Thus, Claim 2 is proven again.]

[4]For example, part **(a)** of this exercise shows that the associativity of multiplication holds for dual numbers; likewise, all the other basic rules can be proven.

We can now finally solve part **(e)** of the exercise:

We have $P(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0 = \sum_{j=0}^{k} a_j x^j$. Substituting a for x in this equation, we find

$$P(a) = \sum_{j=0}^{k} a_j a^j. \tag{7}$$

Moreover, $P'(x) = k a_k x^{k-1} + (k-1) a_{k-1} x^{k-2} + \cdots + 1 a_1 x^0 = \sum_{j=1}^{k} j a_j x^{j-1} = \sum_{j=1}^{k} a_j j x^{j-1}$. Substituting a for x in this equation, we find

$$P'(a) = \sum_{j=1}^{k} a_j j a^{j-1}. \tag{8}$$

Substitute the dual number (a, b) for x in the equation $P(x) = \sum_{j=0}^{k} a_j x^j$. We thus obtain[5]

$$\begin{aligned}
P((a,b)) &= \sum_{j=0}^{k} \underbrace{a_j}_{\substack{=(a_j)_{\mathbb{D}}=(a_j,0) \\ \text{(by the definition} \\ \text{of } (a_j)_{\mathbb{D}})}} \underbrace{(a,b)^j}_{\substack{=\left(a^j, j a^{j-1} b\right) \\ \text{(by Claim 2,} \\ \text{applied to } j \text{ instead of } k)}} = \sum_{j=0}^{k} \underbrace{(a_j, 0) \cdot \left(a^j, j a^{j-1} b\right)}_{\substack{=\left(a_j a^j, a_j j a^{j-1} b + 0 a^j\right) \\ \text{(by the definition} \\ \text{of the operation } \cdot \text{ on } \mathbb{D})}} \\
&= \sum_{j=0}^{k} \left(a_j a^j, \underbrace{a_j j a^{j-1} b + 0 a^j}_{= a_j j a^{j-1} b} \right) = \sum_{j=0}^{k} \left(a_j a^j, j a_j a^{j-1} b \right) = \left(\sum_{j=0}^{k} a_j a^j, \sum_{j=0}^{k} a_j j a^{j-1} b \right) \\
&\qquad \left(\begin{array}{c} \text{by Claim 1, applied to } \{0, 1, \ldots, k\}, \, a_j a^j \text{ and } a_j j a^{j-1} b \\ \text{instead of } J, \, a_j \text{ and } b_j \text{ (since the "} \sum_{j=0}^{k} \text{" sign means "} \sum_{j \in \{0,1,\ldots,k\}} \text{")} \end{array} \right) \\
&= \left(\underbrace{\sum_{j=0}^{k} a_j a^j}_{\substack{=P(a) \\ \text{(by (7))}}}, \underbrace{\sum_{j=1}^{k} a_j j a^{j-1}}_{\substack{=P'(a) \\ \text{(by (8))}}} b \right) \\
&\qquad \left(\text{since } \sum_{j=0}^{k} a_j j a^{j-1} b = a_0 \underbrace{0 a^{0-1}}_{=0} b + \sum_{j=1}^{k} a_j j a^{j-1} b = \sum_{j=1}^{k} a_j j a^{j-1} b \right) \\
&= \left(P(a), \underbrace{P'(a) b}_{=bP'(a)} \right) = (P(a), bP'(a)).
\end{aligned}$$

But part **(b)** of this exercise (applied to $P(a)$ and $bP'(a)$ instead of a and b) yields

$$P(a) + bP'(a)\,\varepsilon = (P(a), bP'(a)). \tag{9}$$

[5]Here, we agree to understand the expression "$j a^{j-1}$" to mean 0 when $j = 0$, even if its sub-expression "a^{j-1}" may be meaningless. This is the same convention that we followed in Claim 2.

But part **(b)** of this exercise yields $a + b\varepsilon = (a, b)$. Hence,

$$P\left(\underbrace{a+b\varepsilon}_{=(a,b)}\right) = P\left((a,b)\right) = \left(P\left(a\right), bP'\left(a\right)\right) = P\left(a\right) + bP'\left(a\right)\varepsilon$$

(by (9)). This solves part **(e)** of the problem.

---

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* $N_2\left(\alpha\right)$ of α by $N_2\left(\alpha\right) = a^2 - 2b^2$, 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 $N_2\left(\alpha\beta\right) = N_2\left(\alpha\right) N_2\left(\beta\right)$ 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 $\mathbb{Z}\left[i\right]$ 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 $\mathbb{Z}\left[i\right]$. 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 $\mathbb{Z}\left[i\right]$, 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

(a) Let $\alpha, \beta \in \mathbb{Z}\left[\sqrt{2}\right]$. We must prove that $\alpha+\beta \in \mathbb{Z}\left[\sqrt{2}\right]$ and $\alpha-\beta \in \mathbb{Z}\left[\sqrt{2}\right]$ and $\alpha\beta \in \mathbb{Z}\left[\sqrt{2}\right]$.

We have $\alpha \in \mathbb{Z}\left[\sqrt{2}\right]$. In other words, α is a real of the form $a+b\sqrt{2}$ with $a, b \in \mathbb{Z}$ (by the definition of $\mathbb{Z}\left[\sqrt{2}\right]$). In other words, there exist two integers $x_1, x_2 \in \mathbb{Z}$ such that $\alpha = x_1 + x_2\sqrt{2}$. Similarly, there exist two integers $y_1, y_2 \in \mathbb{Z}$ such that $\beta = y_1 + y_2\sqrt{2}$. Consider these four integers x_1, x_2, y_1, y_2.

We have

$$\underbrace{\alpha}_{=x_1+x_2\sqrt{2}} + \underbrace{\beta}_{=y_1+y_2\sqrt{2}} = \left(x_1 + x_2\sqrt{2}\right) + \left(y_1 + y_2\sqrt{2}\right) = (x_1+y_1) + (x_2+y_2)\sqrt{2}.$$

Hence, $\alpha+\beta$ is a real of the form $a+b\sqrt{2}$ with $a, b \in \mathbb{Z}$ (namely, with $a = x_1+y_1$ and $b = x_2+y_2$). In other words, $\alpha+\beta \in \mathbb{Z}\left[\sqrt{2}\right]$ (by the definition of $\mathbb{Z}\left[\sqrt{2}\right]$).

We have

$$\underbrace{\alpha}_{=x_1+x_2\sqrt{2}} - \underbrace{\beta}_{=y_1+y_2\sqrt{2}} = \left(x_1 + x_2\sqrt{2}\right) - \left(y_1 + y_2\sqrt{2}\right) = (x_1-y_1) + (x_2-y_2)\sqrt{2}.$$

Hence, $\alpha-\beta$ is a real of the form $a+b\sqrt{2}$ with $a, b \in \mathbb{Z}$ (namely, with $a = x_1-y_1$ and $b = x_2-y_2$). In other words, $\alpha-\beta \in \mathbb{Z}\left[\sqrt{2}\right]$ (by the definition of $\mathbb{Z}\left[\sqrt{2}\right]$).

We have

$$\begin{aligned}
\underbrace{\alpha}_{=x_1+x_2\sqrt{2}}\underbrace{\beta}_{=y_1+y_2\sqrt{2}} &= \left(x_1 + x_2\sqrt{2}\right)\left(y_1 + y_2\sqrt{2}\right) = x_1y_1 + x_1y_2\sqrt{2} + x_2\sqrt{2}y_1 + x_2\sqrt{2}y_2\sqrt{2} \\
&= x_1y_1 + x_1y_2\sqrt{2} + x_2\underbrace{\sqrt{2}y_1}_{=y_1\sqrt{2}} + x_2\underbrace{\sqrt{2}y_2}_{=y_2\sqrt{2}}\sqrt{2} \\
&= x_1y_1 + x_1y_2\sqrt{2} + x_2y_1\sqrt{2} + x_2y_2\underbrace{\sqrt{2}\sqrt{2}}_{=\left(\sqrt{2}\right)^2=2} \\
&= x_1y_1 + x_1y_2\sqrt{2} + x_2y_1\sqrt{2} + x_2y_2 2 \\
&= (x_1y_1 + 2x_2y_2) + (x_1y_2 + x_2y_1)\sqrt{2}. \qquad (10)
\end{aligned}$$

Hence, $\alpha\beta$ is a real of the form $a+b\sqrt{2}$ with $a, b \in \mathbb{Z}$ (namely, with $a = x_1y_1 + 2x_2y_2$ and $b = x_1y_2 + x_2y_1$). In other words, $\alpha\beta \in \mathbb{Z}\left[\sqrt{2}\right]$ (by the definition of $\mathbb{Z}\left[\sqrt{2}\right]$).

We have now shown that $\alpha+\beta \in \mathbb{Z}\left[\sqrt{2}\right]$ and $\alpha-\beta \in \mathbb{Z}\left[\sqrt{2}\right]$ and $\alpha\beta \in \mathbb{Z}\left[\sqrt{2}\right]$. This solves part **(a)** of the exercise.

(b) Let α be an element of $\mathbb{Z}\left[\sqrt{2}\right]$. We must prove that α can be written as $a+b\sqrt{2}$ for a **unique** pair (a, b) of integers.

Clearly, α can be written as $a+b\sqrt{2}$ for **at least one** pair (a, b) of integers (because this is what it means for α to belong to $\mathbb{Z}\left[\sqrt{2}\right]$). Thus, it remains to prove that α can be written as $a+b\sqrt{2}$ for **at most one** pair (a, b) of integers. In other words, we must prove that if (a_1, b_1) and (a_2, b_2) are two pairs (a, b) of integers such that $\alpha = a+b\sqrt{2}$, then $(a_1, b_1) = (a_2, b_2)$.

Let us prove this. Let (a_1, b_1) and (a_2, b_2) be two pairs (a, b) of integers such that $\alpha = a+b\sqrt{2}$. We must show that $(a_1, b_1) = (a_2, b_2)$.

Assume the contrary. Thus, $(a_1, b_1) \neq (a_2, b_2)$.

It is easy to check that 2 is not a perfect square. (We can show something more general: Any integer that is congruent to 2 or 3 modulo 4 is not a perfect square. Indeed, Exercise 2.7.2 in the class notes shows that each integer u satisfies either $u^2 \equiv 0 \bmod 4$ (if u is even) or $u^2 \equiv 1 \bmod 4$ (if u is odd). In other words, each perfect square is congruent to either 0 or 1 modulo 4. Thus, any integer that is congruent to 2 or 3 modulo 4 is not a perfect square.)

Exercise 2.10.15 **(a)** in the class notes shows that if a positive integer u is not a perfect square, then $\sqrt{u}$ is irrational. Applying this to $u = 2$, we conclude that $\sqrt{2}$ is irrational (since 2 is not a perfect square).

But (a_1, b_1) is a pair (a, b) of integers such that $\alpha = a + b\sqrt{2}$. In other words, (a_1, b_1) is a pair of integers and satisfies $\alpha = a_1 + b_1\sqrt{2}$. Similarly, (a_2, b_2) is a pair of integers and satisfies $\alpha = a_2 + b_2\sqrt{2}$. Hence, $a_2 + b_2\sqrt{2} = \alpha = a_1 + b_1\sqrt{2}$, so that

$$a_2 - a_1 = b_1\sqrt{2} - b_2\sqrt{2} = (b_1 - b_2)\sqrt{2}. \tag{11}$$

If we had $b_1 = b_2$, then this would yield $a_2 - a_1 = \underbrace{(b_1 - b_2)}_{\substack{=0 \\ (\text{since } b_1 = b_2)}}\sqrt{2} = 0$, which would lead to $a_1 = a_2$ and therefore $\left(\underbrace{a_1}_{=a_2}, \underbrace{b_1}_{=b_2}\right) = (a_2, b_2)$; but this would contradict $(a_1, b_1) \neq (a_2, b_2)$. Hence, we cannot have $b_1 = b_2$. Thus, we have $b_1 \neq b_2$. In other words, $b_1 - b_2 \neq 0$. Hence, we can divide both sides of the equality (11) by $b_1 - b_2$. We thus obtain $\dfrac{a_2 - a_1}{b_1 - b_2} = \sqrt{2}$. Hence, the number $\dfrac{a_2 - a_1}{b_1 - b_2}$ is irrational (since $\sqrt{2}$ is irrational). But this contradicts the fact that $\dfrac{a_2 - a_1}{b_1 - b_2}$ is rational (which is clear, since a_1, a_2, b_1, b_2 are integers). This contradiction shows that our assumption was wrong. Hence, $(a_1, b_1) = (a_2, b_2)$ is proven. This completes our solution of part **(b)** of the exercise.

(c) Let $\alpha, \beta \in \mathbb{Z}\left[\sqrt{2}\right]$. We must prove that $N_2(\alpha\beta) = N_2(\alpha)\, N_2(\beta)$.

We have $\alpha \in \mathbb{Z}\left[\sqrt{2}\right]$. In other words, α is a real of the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$ (by the definition of $\mathbb{Z}\left[\sqrt{2}\right]$). In other words, there exist two integers $x_1, x_2 \in \mathbb{Z}$ such that $\alpha = x_1 + x_2\sqrt{2}$. Similarly, there exist two integers $y_1, y_2 \in \mathbb{Z}$ such that $\beta = y_1 + y_2\sqrt{2}$. Consider these four integers x_1, x_2, y_1, y_2.

We have $\alpha = x_1 + x_2\sqrt{2}$ with $x_1, x_2 \in \mathbb{Z}$. Thus, the definition of $N_2(\alpha)$ yields $N_2(\alpha) = x_1^2 - 2x_2^2$. Similarly, $N_2(\beta) = y_1^2 - 2y_2^2$. But (10) shows that

$$\alpha\beta = (x_1y_1 + 2x_2y_2) + (x_1y_2 + x_2y_1)\sqrt{2} \qquad \text{with } x_1y_1 + 2x_2y_2, x_1y_2 + x_2y_1 \in \mathbb{Z}.$$

Hence, the definition of $N_2(\alpha\beta)$ yields

$$N_2(\alpha\beta) = (x_1y_1 + 2x_2y_2)^2 - 2(x_1y_2 + x_2y_1)^2 = x_1^2y_1^2 - 2x_1^2y_2^2 - 2x_2^2y_1^2 + 4x_2^2y_2^2$$

(after some straightforward computation). Comparing this with

$$\underbrace{N_2(\alpha)}_{=x_1^2 - 2x_2^2}\underbrace{N_2(\beta)}_{=y_1^2 - 2y_2^2} = \left(x_1^2 - 2x_2^2\right)\left(y_1^2 - 2y_2^2\right) = x_1^2y_1^2 - 2x_1^2y_2^2 - 2x_2^2y_1^2 + 4x_2^2y_2^2,$$

we obtain $N_2(\alpha\beta) = N_2(\alpha)\, N_2(\beta)$. This solves part **(c)** of the exercise.

[*Remark:* An alternative solution to part **(c)** relies on the concept of a $\sqrt{2}$-conjugate of an $\alpha \in \mathbb{Z}\left[\sqrt{2}\right]$. Namely, the *$\sqrt{2}$-conjugate* of an $\alpha \in \mathbb{Z}\left[\sqrt{2}\right]$ is defined to be the number $a - b\sqrt{2}$, where α is written in the form $\alpha = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. We denote this $\sqrt{2}$-conjugate by $\overline{\alpha}$, but keep in mind that this notation clashes with the notation $\overline{\alpha}$ for complex numbers α. (Fortunately, we will not talk about complex numbers in this solution, so this clash does not matter.) It is easy to see that $N_2(\alpha) = \alpha\overline{\alpha}$ for each $\alpha \in \mathbb{Z}\left[\sqrt{2}\right]$, and it is also easy to see that $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$ for any $\alpha, \beta \in \mathbb{Z}\left[\sqrt{2}\right]$. Armed with these two equalities, we can now observe that any $\alpha, \beta \in \mathbb{Z}\left[\sqrt{2}\right]$ satisfy

$$N_2(\alpha\beta) = \alpha\beta \cdot \underbrace{\overline{\alpha\beta}}_{=\overline{\alpha}\cdot\overline{\beta}} = \alpha\beta \cdot \overline{\alpha} \cdot \overline{\beta} = \underbrace{\alpha\overline{\alpha}}_{=N_2(\alpha)} \underbrace{\beta\overline{\beta}}_{=N_2(\beta)} = N_2(\alpha) N_2(\beta).$$

This solves part **(c)** of the exercise again.]

(d) We shall solve part **(d)** of the exercise by induction on n:

Induction base: We have $p_2 \underbrace{p_0}_{=0} - p_1^2 = p_2 0 - p_1^2 = -p_1^2 = -1^2$ (since $p_1 = 1$). Thus, $p_2 p_0 - p_1^2 = -1^2 = -1 = (-1)^1$. In other words, part **(d)** of the exercise holds for $n = 1$. This completes the induction base.

Induction step: Let $m \geq 1$ be an integer. Assume that part **(d)** of the exercise holds for $n = m$. We must prove that part **(d)** of the exercise holds for $n = m + 1$.

We have assumed that part **(d)** of the exercise holds for $n = m$. In other words, $p_{m+1} p_{m-1} - p_m^2 = (-1)^m$.

The recursive definition of the sequence $(p_0, p_1, p_2, \ldots)$ yields $p_{m+2} = 2p_{m+1} + p_m$ and $p_{m+1} = 2p_m + p_{m-1}$. From $p_{m+1} = 2p_m + p_{m-1}$, we obtain $2p_m - \underbrace{p_{m+1}}_{=2p_m+p_{m-1}} = 2p_m - (2p_m + p_{m-1}) = -p_{m-1}$. Now,

$$\begin{aligned} \underbrace{p_{m+2}}_{=2p_{m+1}+p_m} p_m - p_{m+1}^2 &= (2p_{m+1} + p_m) p_m - p_{m+1}^2 = 2p_{m+1}p_m + p_m^2 - p_{m+1}^2 \\ &= p_{m+1} \underbrace{(2p_m - p_{m+1})}_{=-p_{m-1}} + p_m^2 = p_{m+1}(-p_{m-1}) + p_m^2 \\ &= -\underbrace{\left(p_{m+1}p_{m-1} - p_m^2\right)}_{=(-1)^m} = -(-1)^m = (-1)^{m+1}. \end{aligned}$$

In other words, part **(d)** of the exercise holds for $n = m + 1$. This completes the induction step. Thus, part **(d)** of the exercise is proven by induction.

(e) Let $n \geq 1$. The recursive definition of the sequence $(p_0, p_1, p_2, \ldots)$ yields $p_{n+1} = 2p_n + p_{n-1}$.

Recall the classical identity $(a + b)(a - b) = a^2 - b^2$, which holds for any reals a and b.

Applying this to $a = p_{n-1} + p_n$ and $b = p_n\sqrt{2}$, we obtain

$$\begin{aligned}
&\left(p_{n-1} + p_n + p_n\sqrt{2}\right)\left(p_{n-1} + p_n - p_n\sqrt{2}\right) \\
&= \underbrace{\left(p_{n-1} + p_n\right)^2}_{=p_{n-1}^2+2p_{n-1}p_n+p_n^2} - \underbrace{\left(p_n\sqrt{2}\right)^2}_{=p_n^2\cdot 2=2p_n^2} = p_{n-1}^2 + 2p_{n-1}p_n + p_n^2 - 2p_n^2 = 2p_{n-1}p_n + p_{n-1}^2 - p_n^2 \\
&= p_{n-1}\underbrace{\left(2p_n + p_{n-1}\right)}_{=p_{n+1}} - p_n^2 = p_{n-1}p_{n+1} - p_n^2 = p_{n+1}p_{n-1} - p_n^2 = (-1)^n
\end{aligned}$$

(by part **(d)** of the exercise). This solves part **(e)** of the exercise.

4.4 Remark

Let r be any nonnegative real number.

Part **(a)** of this exercise remains valid if we replace each appearance of "2" by "r". (We could even allow r to be negative, if we also replace "reals" by "complex numbers".)

Parts **(b)** and **(c)** of this exercise remain valid if we replace each appearance of "2" by "r", provided that r is a positive integer that is not a perfect square. (Of course, the $\sqrt{2}$-norm $N_2(\alpha)$ needs to be replaced by the $\sqrt{r}$-norm $N_r(\alpha)$, defined by setting $N_r(\alpha) = a^2 - rb^2$ for $\alpha = a + b\sqrt{r}$.)

All three parts **(a)**, **(b)** and **(c)** of this exercise remain valid if we replace integers by rational numbers throughout (i.e., we consider the set of reals of the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ instead of $a, b \in \mathbb{Z}$).

Part **(d)** of this exercise remains valid if we replace each appearance of "2" by "r". (Again, we could even allow r to be negative.) Note that if we set $r = 1$, then the sequence $(p_0, p_1, p_2, \ldots)$ becomes the famous Fibonacci sequence $(0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots)$.

Part **(e)**, on the other hand, hinges on the specific properties of $\sqrt{2}$.

---

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

See the class notes, where this is Exercise 2.16.3. (The numbering may shift; it is one of the exercises in the "The Chinese Remainder Theorem as a bijection" section.)

---

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

See the class notes, where this is Exercise 2.15.5. (The numbering may shift; it is one of the exercises in the "Fermat, Euler, Wilson" section.)