University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Midterm 3

Darij Grinberg

May 15, 2019

due date: **Monday, 6 May 2019 at 20:00** on Canvas or by email.
No collaboration allowed – this is a midterm.
Please solve **at most 3 of the 6 exercises**!

1 Exercise 1: Nonunital rings and local unities

1.1 Problem

A *nonunital ring* is defined in the same way as we defined a ring, except that we don't require it to be endowed with an element 1 (and, correspondingly, we omit the "Neutrality of one" axiom). This does not mean that a nonunital ring must not contain an element 1 that would satisfy the "Neutrality of one" axiom; it simply means that such an element is not required (and not considered part of the ring structure). So, formally speaking, a nonunital ring is a 4-tuple $(\mathbb{K}, +, \cdot, 0)$ (while a ring in the usual sense is a 5-tuple $(\mathbb{K}, +, \cdot, 0, 1)$) that satisfies all the ring axioms except for "Neutrality of one".

Thus, every ring becomes a nonunital ring if we forget its unity (i.e., if $(\mathbb{K}, +, \cdot, 0, 1)$ is a ring, then $(\mathbb{K}, +, \cdot, 0)$ is a nonunital ring). But there are other examples as well: For instance, if $n \in \mathbb{Z}$ is arbitrary, then $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\} = \{\text{all multiples of } n\}$ is a nonunital ring (when endowed with the usual $+$, $\cdot$ and 0).

An element z of a nonunital ring $\mathbb{K}$ is said to be a *unity* of $\mathbb{K}$ if every $a \in \mathbb{K}$ satisfies $az = za = a$. In other words, an element z of a nonunital ring $\mathbb{K}$ is said to be a *unity* of $\mathbb{K}$ if equipping $\mathbb{K}$ with the unity z results in a ring (in the usual sense of this word).

Prove the following:

(a) If $n \in \mathbb{Z}$, then the nonunital ring $n\mathbb{Z}$ has a unity if and only if $n \in \{1, 0, -1\}$.

(b) Any nonunital ring has **at most one** unity.

Now, let $\mathbb{K}$ be a nonunital ring. As usual, we write $+$ and $\cdot$ for its two operations, and 0 for its zero.

Let $z \in \mathbb{K}$. Define a subset U_z of $\mathbb{K}$ by

$$U_z = \{r \in \mathbb{K} \mid rz = zr = r\}.$$

(c) Prove that $0 \in U_z$, and that every $a, b \in U_z$ satisfy $a + b \in U_z$ and $ab \in U_z$.

Thus, we can turn U_z into a nonunital ring by endowing U_z with the binary operations $+$ and $\cdot$ (inherited from $\mathbb{K}$) and the element 0. Consider this nonunital ring U_z.

(d) Assume that $z^2 = z$. Prove that z is a unity of the nonunital ring U_z.

[**Hint:** In **(b)**, what would the product of two unities be?]

1.2 Solution

[...]

---

2 Exercise 2: Rings from nonunital rings

2.1 Problem

Let $\mathbb{K}$ be a nonunital ring. (See Exercise 1 for the definition of this notion.) Let $\mathbb{L}$ be the Cartesian product $\mathbb{Z} \times \mathbb{K}$ (so far, just a set). Define a binary operation $+$ on $\mathbb{L}$ by setting

$$(n, a) + (m, b) = (n + m, a + b) \qquad \text{for all } (n, a), (m, b) \in \mathbb{L}.$$

(This is an entrywise addition.) Define a binary operation $\cdot$ on $\mathbb{L}$ by

$$(n, a)(m, b) = (nm, nb + ma + ab) \qquad \text{for all } (n, a), (m, b) \in \mathbb{L}.$$

(Here, nb and ma are defined in the usual way: If $n \in \mathbb{Z}$ and $a \in \mathbb{K}$, then $na \in \mathbb{K}$ is defined by

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a + a + \cdots + a}_{-n \text{ times}}\right), & \text{if } n < 0 \end{cases}.$$

This does not require $\mathbb{K}$ to have a unity.)

Prove that $\mathbb{L}$, endowed with these two operations $+$ and $\cdot$ and the zero $(0, 0)$ and the unity $(1, 0)$, is a ring (in the usual sense of this word).

[**Hint:** You can use rules like $n(a + b) = na + nb$ and $(n + m)a = na + ma$ and $(nm)a = n(ma)$ (for $n, m \in \mathbb{Z}$ and $a, b \in \mathbb{K}$) without proof; they can be proven just as for usual rings. You can also use the fact that finite sums of elements of $\mathbb{K}$ are well-defined and

behave as we would expect them to (we already tacitly used that in writing "$\underbrace{a+a+\cdots+a}_{n \text{ times}}$" without parentheses).

You don't need to check the "additive" axioms (associativity of addition, commutativity of addition, neutrality of zero, and existence of additive inverses); as far as addition and zero are concerned, $\mathbb{L}$ is just a Cartesian product.]

2.2 Remark

This exercise gives a way to "embed" any nonunital ring $\mathbb{K}$ into a ring $\mathbb{L}$. This helps proving properties of nonunital rings, assuming that you can prove them for rings.

There is also a much simpler notion of a Cartesian product of two nonunital rings (in which both addition and multiplication are defined entrywise). This lets us define a nonunital ring $\mathbb{Z} \times \mathbb{K}$. But this is **not** the ring $\mathbb{L}$; it does not generally have a unity.

2.3 Solution

[...]

---

3 Exercise 3: More sums from number theory

3.1 Problem

(a) Let n be a positive integer. Prove that

$$\sum_{j=1}^{n} \gcd(j,n) = \sum_{d \mid n} d\phi\left(\frac{n}{d}\right).$$

More generally, if $(a_1, a_2, a_3, \ldots)$ is a sequence of reals, then prove that

$$\sum_{j=1}^{n} a_{\gcd(j,n)} = \sum_{d \mid n} a_d \phi\left(\frac{n}{d}\right).$$

(b) Let $n \in \mathbb{N}$. Prove that

$$\begin{aligned}
&\left(\text{the number of } (x,y) \in \mathbb{Z}^2 \text{ satisfying } x^2+y^2 \leq n\right) \\
&= 1 + 4\sum_{k \in \mathbb{N}} (-1)^k \left\lfloor \frac{n}{2k+1} \right\rfloor \\
&= 1 + 4\left(\left\lfloor \frac{n}{1} \right\rfloor - \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{5} \right\rfloor - \left\lfloor \frac{n}{7} \right\rfloor + \left\lfloor \frac{n}{9} \right\rfloor - \left\lfloor \frac{n}{11} \right\rfloor \pm \cdots\right).
\end{aligned}$$

(The infinite sums in this equality have only finitely many nonzero addends, and thus are well-defined.)

[**Hint:** Parts **(a)** and **(b)** have nothing to do with each other.

This is a good place for a reminder that results proven in the notes, as well as problems from previous homework sets and midterms, can be freely used. Both parts have rather short solutions if you remember the right results to use!]

3.2 Remark

Part **(b)** of this exercise is a "discrete" version of the famous Madhava–Gregory–Leibniz series

$$\frac{\pi}{4} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} \pm \cdots$$

(where π, at last, does denote the area of the unit circle). Indeed, if we divide the number of $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 + y^2 \leq n$ by n, then we obtain an approximation to the area of the unit circle that gets better as n grows[1]. On the other hand, it appears reasonable that dividing

$$1 + 4\left(\left\lfloor \frac{n}{1} \right\rfloor - \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{5} \right\rfloor - \left\lfloor \frac{n}{7} \right\rfloor + \left\lfloor \frac{n}{9} \right\rfloor - \left\lfloor \frac{n}{11} \right\rfloor \pm \cdots\right)$$

by n, we obtain an approximation to $4\left(\frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} \pm \cdots\right)$. I am not sure whether this can be rigorously proven, however.[2]

3.3 Solution

[...]

---

4 Exercise 4: Squares in finite fields II

4.1 Problem

Let $\mathbb{F}$ be a finite field such that $2 \cdot 1_{\mathbb{F}} \neq 0_{\mathbb{F}}$. In Exercise 5 of homework set #6, we have seen that $|\mathbb{F}|$ is odd, and that the number of squares in $\mathbb{F}$ is $\frac{1}{2}(|\mathbb{F}| + 1)$.

In the following, the word "square" shall always mean "square in $\mathbb{F}$".

A *nonsquare* shall mean an element of $\mathbb{F}$ that is not a square.

Prove the following:

(a) The product of two squares is always a square.

(b) The product of a nonzero square with a nonsquare is always a nonsquare.

(c) The product of two nonsquares is always a square.

[**Hint:** It is easiest to solve the three parts in this exact order. For **(c)**, recall that if a subset Y of a finite set X satisfies $|Y| \geq |X|$, then $Y = X$.]

[1] Just observe that the pairs $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 + y^2 \leq n$, regarded as points in the Euclidean plane, are precisely the lattice points inside the circle with center 0 and radius $\sqrt{n}$. Thus, by counting these pairs, we are approximating the area of this circle. See [Clark18, Theorem 12.1] for a rigorous proof.

[2] Of course, for any given $k \in \mathbb{N}$, the number $\frac{1}{n}\left(\left\lfloor \frac{n}{2k+1} \right\rfloor - \frac{n}{2k+1}\right)$ does converge to 0 when $n \to \infty$. But here we are taking an alternating sum of infinitely many such numbers; we can ignore all but the first n, but even the first n may no longer converge to 0 when summed together.

4.2 Solution

[...]

---

5 Exercise 5: Formal differential calculus

5.1 Problem

Let $\mathbb{K}$ be a commutative ring. For each FPS[3]

$$f = \sum_{k \in \mathbb{N}} a_k x^k = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots \in \mathbb{K}\left[\left[x\right]\right] \qquad \left(\text{where } a_i \in \mathbb{K}\right),$$

we define the *derivative* f' of f to be the FPS

$$\sum_{k>0} k a_k x^{k-1} = 1a_1 x^0 + 2a_2 x^1 + 3a_3 x^2 + \cdots \in \mathbb{K}\left[\left[x\right]\right].$$

(This definition imitates the standard procedure for differentiating power series in analysis, but it does not require any analysis or topology itself. In particular, $\mathbb{K}$ may be any commutative ring – e.g., a finite field.)

Let $D : \mathbb{K}\left[\left[x\right]\right] \to \mathbb{K}\left[\left[x\right]\right]$ be the map sending each FPS f to its derivative f'. We refer to D as *(formal) differentiation*. As usual, for any $n \in \mathbb{N}$, we let D^n denote $\underbrace{D \circ D \circ \cdots \circ D}_{n \text{ times}}$ (which means id if $n = 0$).

Prove the following:

(a) If $f \in \mathbb{K}\left[x\right]$, then $f' \in \mathbb{K}\left[x\right]$ and $\deg\left(f'\right) \leq \deg f - 1$. (In other words, the derivative of a polynomial is again a polynomial of degree at least 1 less.)

(b) The map $D : \mathbb{K}\left[\left[x\right]\right] \to \mathbb{K}\left[\left[x\right]\right]$ is $\mathbb{K}$-linear (with respect to the $\mathbb{K}$-module structure on $\mathbb{K}\left[\left[x\right]\right]$ defined in class – i.e., both addition and scaling of FPSs are defined entrywise).

(c) We have $\left(fg\right)' = f'g + fg'$ for any two FPSs f and g. (This is called the *Leibniz rule*.)

(d) We have $D^n\left(x^k\right) = n!\dbinom{k}{n} x^{k-n}$ for all $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Here, the expression "$\dbinom{k}{n} x^{k-n}$" is to be understood as 0 when $k < n$.

(e) If $\mathbb{Q}$ is a subring of $\mathbb{K}$, then every polynomial $f \in \mathbb{K}\left[x\right]$ satisfies[4]

$$f\left[x + a\right] = \sum_{n \in \mathbb{N}} \frac{1}{n!} \left(D^n\left(f\right)\right)\left[a\right] \cdot x^n \qquad \text{for all } a \in \mathbb{K}.$$

(The infinite sum on the right hand side has only finitely many nonzero addends.)

[3] Just as in class, the abbreviation "FPS" stands for "formal power series". All FPSs and polynomials in this exercise are in 1 indeterminate over $\mathbb{K}$; the indeterminate is called x.

[4] Just as in class, I am using the notation "$f\left[u\right]$" for the evaluation of f at u. The more common notation for this is $f\left(u\right)$, but is too easily mistaken for a product.
Note also that we need to require f to be a polynomial here, since $f\left[x + a\right]$ would not be defined if f was merely an FPS.

(f) If p is a prime such that $p \cdot 1_{\mathbb{K}} = 0$ (for example, this happens if $\mathbb{K} = \mathbb{Z}/p$), then $D^p(f) = 0$ for each $f \in \mathbb{K}[[x]]$.

Now, assume that $\mathbb{Q}$ is a subring of $\mathbb{K}$. For each FPS

$$f = \sum_{k \in \mathbb{N}} a_k x^k = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots \in \mathbb{K}[[x]] \qquad (\text{where } a_i \in \mathbb{K}),$$

we define the *integral* $\int f$ of f to be the FPS

$$\sum_{k \geq 0} \frac{1}{k+1} a_k x^{k+1} = \frac{1}{1} a_0 x^1 + \frac{1}{2} a_1 x^2 + \frac{1}{3} a_2 x^3 + \cdots \in \mathbb{K}[[x]].$$

(This definition imitates the standard procedure for integrating power series in analysis, but again works for any commutative ring $\mathbb{K}$ that contains $\mathbb{Q}$ as subring.)

Let $J : \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ be the map sending each FPS f to its integral $\int f$. Prove the following:

(g) The map $J : \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ is $\mathbb{K}$-linear.

(h) We have $D \circ J = \mathrm{id}$.

(i) We have $J \circ D \neq \mathrm{id}$.

[**Hint:** Don't give too much detail; workable outlines are sufficient. Feel free to interchange summation signs without justification. For part **(c)**, it is easiest to first prove it in the particular case when $f = x^a$ and $g = x^b$ for some f and g, and then obtain the general case by interchanging summations.]

5.2 Remark

This exercise is just the beginning of "algebraic calculus". A lot more can be done: Differentiation can be extended to rational functions; partial derivatives can be defined for multivariate polynomials and FPSs; differential equations can be solved formally in FPSs (rather than functions); even a purely algebraic analogue of the classical $f'(x) = \lim\limits_{\varepsilon \to 0} \dfrac{f(x+\varepsilon) - f(x)}{\varepsilon}$ definition exists[5]. These algebraic derivatives play crucial roles in the study of fields (including finite fields!), in algebraic geometry (where they help define what a "singularity" of an algebraic variety is) and in enumerative combinatorics (where they aid in computing generating functions).

Part **(e)** is perhaps the easiest instance of the well-known Taylor formula (no error terms, no smoothness requirements, no convergence issues).

The "integral" $\int f$ we defined above is, of course, only one possible choice of an FPS g satisfying $g' = f$. Just as in calculus, you can add any constant to it, and you get another. Part **(h)** is an algebraic version of one half of the Fundamental Theorem of Calculus. You can easily prove the other half: For each FPS f, the FPS $(J \circ D)(f)$ differs from f only in its constant term.

If $\mathbb{K}$ contains $\mathbb{Q}$ as a subring, then both J and D are elements of the $\mathbb{K}$-algebra $\mathrm{End}(\mathbb{K}[[x]])$ (by parts **(b)** and **(g)** of this exercise). Part **(h)** of this exercise shows that J is a right inverse of D; but part **(i)** shows that J is not a left inverse (and thus not an inverse) of D. This yields an example of a left inverse that is not a right inverse.

[5] See Theorem 5 in `https://math.stackexchange.com/a/2974977/` .

5.3 Solution

[...]

---

6 Exercise 6: Formal difference calculus and integer-valued polynomials

6.1 Problem

Let $\mathbb{K}$ be a commutative ring.

For any polynomial $f \in \mathbb{K}[x]$, we define the *first finite difference* f^{Δ} of f to be the polynomial

$$f[x+1] - f[x] \in \mathbb{K}[x].$$

(This is a "discrete analogue" of the derivative, in case the analysis-free derivative from Exercise 5 was not discrete enough for you. It cannot be extended to FPSs, however, since you cannot substitute $x+1$ for x in an FPS.)

Let $\Delta : \mathbb{K}[x] \to \mathbb{K}[x]$ be the map sending each polynomial f to f^{Δ}. As usual, for any $n \in \mathbb{N}$, we let Δ^n denote $\underbrace{\Delta \circ \Delta \circ \cdots \circ \Delta}_{n \text{ times}}$ (which means id if $n = 0$).

Prove the following:

(a) The map $\Delta : \mathbb{K}[x] \to \mathbb{K}[x]$ is $\mathbb{K}$-linear (with respect to the $\mathbb{K}$-module structure on $\mathbb{K}[x]$ defined in class – i.e., both addition and scaling of polynomials are defined entrywise).

(b) We have $(fg)^{\Delta} = f^{\Delta} g + f[x+1]\, g^{\Delta}$ for any two polynomials f and g.

Now, assume that $\mathbb{Q}$ is a subring of $\mathbb{K}$.

For any $n \in \mathbb{N}$, we define a polynomial[6]

$$\binom{x}{n} := \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!} \in \mathbb{K}[x].$$

We also set $\binom{x}{n} := 0$ for every negative n.

Prove the following:

(c) We have $\Delta^n\left(\binom{x}{k}\right) = \binom{x}{k-n}$ for all $n \in \mathbb{N}$ and $k \in \mathbb{Z}$.

(d) If $m \in \mathbb{N}$, and if $f \in \mathbb{K}[x]$ is a polynomial of degree $\leq m$, then there exist elements $a_0, a_1, \ldots, a_m \in \mathbb{K}$ such that $f = \sum_{i=0}^{m} a_i \binom{x}{i}$.

(e) Every polynomial $f \in \mathbb{K}[x]$ satisfies

$$f[x+a] = \sum_{n \in \mathbb{N}} \left(\Delta^n(f)\right)[a] \cdot \binom{x}{n} \qquad \text{for all } a \in \mathbb{K}.$$

(The infinite sum on the right hand side has only finitely many nonzero addends.)

[6]Note that we are within our rights to divide by $n!$ here, since $\mathbb{Q}$ is a subring of $\mathbb{K}$.

(f) Let $m \in \mathbb{N}$, and let $f \in \mathbb{K}[x]$ be a polynomial of degree $\leq m$. Assume that $f[k] \in \mathbb{Z}$ for each $k \in \{0, 1, \ldots, m\}$. Then, there exist integers $a_0, a_1, \ldots, a_m$ such that $f = \sum_{i=0}^{m} a_i \binom{x}{i}$.

[**Hint:** Part **(d)** is easiest to prove by induction on m. You can then prove part **(e)** for $f = \binom{x}{i}$ first (where $i \in \mathbb{N}$), and then extend it to arbitrary f by means of part **(d)**. Part **(f)**, in turn, can be derived from part **(e)** through a strategic choice of a.]

6.2 Remark

Just as Δ is an analogue of the differentiation operator D from Exercise 5, we can define an analogue of the integration operator J from Exercise 5. This will be a $\mathbb{K}$-linear map $\Sigma : \mathbb{K}[x] \to \mathbb{K}[x]$ that sends each polynomial $\sum_{i=0}^{m} a_i \binom{x}{i}$ to $\sum_{i=0}^{m} a_i \binom{x}{i+1}$ (this definition makes sense, because part **(d)** of this exercise shows that each polynomial can be written in the form $\sum_{i=0}^{m} a_i \binom{x}{i}$, uniquely except for "leading zeroes"). Again, we have $\Delta \circ \Sigma = \mathrm{id}$ but $\Sigma \circ \Delta \neq \mathrm{id}$.

Moreover, if $f \in \mathbb{K}[x]$ is a polynomial, then $(\Sigma(f))[0] = 0$ and $(\Sigma(f))[n] = (\Sigma(f))[n-1] + f[n-1]$ for each $n \in \mathbb{Z}$ (indeed, the former equality follows easily from the definition of Σ, while the latter follows from $\Delta \circ \Sigma = \mathrm{id}$). Hence, by induction, we can see that

$$(\Sigma(f))[n] = f[0] + f[1] + \cdots + f[n-1] \qquad \text{for each polynomial } f \in \mathbb{K}[x] \text{ and each } n \in \mathbb{N}.$$

In other words, the value of $\Sigma(f)$ at an $n \in \mathbb{N}$ is the sum of the first n values of f on nonnegative integers! (Whence the notation Σ.) For example, if we set $f = x^2$, then it is easy to see that $\Sigma(f) = 2\binom{x}{3} + \binom{x}{2}$ (to see this, just expand f in the form $\sum_{i=0}^{m} a_i \binom{x}{i}$ – namely, $f = x^2 = 2\binom{x}{2} + \binom{x}{1}$ –, and then apply the definition of Σ); thus we obtain

$$2\binom{n}{3} + \binom{n}{2} = 0^2 + 1^2 + \cdots + (n-1)^2.$$

Similarly you can find a formula for $0^k + 1^k + \cdots + (n-1)^k$ whenever $k \in \mathbb{N}$.

Part **(e)** of this exercise is a result of Newton.

6.3 Solution

[...]

References

[Clark18] Pete L. Clark, *Number Theory: A Contemporary Introduction*, 8 January 2018. `http://math.uga.edu/~pete/4400FULL.pdf`