University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Homework 6

Darij Grinberg

May 15, 2019

due date: **by Canvas or email till the beginning of class on Monday, 22 April 2019**.
Please solve **at most 3 of the 6 exercises**!

1 Exercise 1: The opposite ring

Let $\mathbb{K}$ be a ring. We define a new binary operation $\widetilde{\cdot}$ on $\mathbb{K}$ by setting

$$a \mathbin{\widetilde{\cdot}} b = ba \qquad \text{for all } a, b \in \mathbb{K}.$$

(Thus, $\widetilde{\cdot}$ is the multiplication of $\mathbb{K}$, but with the arguments switched.)

(a) Prove that the set $\mathbb{K}$, equipped with the addition $+$, the multiplication $\widetilde{\cdot}$, the zero $0_{\mathbb{K}}$ and the unity $1_{\mathbb{K}}$, is a ring.

This new ring is called the *opposite ring* of $\mathbb{K}$, and is denoted by $\mathbb{K}^{\mathrm{op}}$.

Note that the **sets** $\mathbb{K}$ and $\mathbb{K}^{\mathrm{op}}$ are identical (so a map from $\mathbb{K}$ to $\mathbb{K}$ is the same as a map from $\mathbb{K}$ to $\mathbb{K}^{\mathrm{op}}$); but the **rings** $\mathbb{K}$ and $\mathbb{K}^{\mathrm{op}}$ are generally not the same (so a ring homomorphism from $\mathbb{K}$ to $\mathbb{K}$ is not the same as a ring homomorphism from $\mathbb{K}$ to $\mathbb{K}^{\mathrm{op}}$).

(b) Prove that the identity map $\mathrm{id} : \mathbb{K} \to \mathbb{K}$ is a ring isomorphism from $\mathbb{K}$ to $\mathbb{K}^{\mathrm{op}}$ if and only if $\mathbb{K}$ is commutative.

(c) Now, assume that $\mathbb{K}$ is the matrix ring $\mathbb{L}^{n\times n}$ for some commutative ring $\mathbb{L}$ and some $n \in \mathbb{N}$. Prove that the map

$$\mathbb{K} \to \mathbb{K}^{\mathrm{op}}, \qquad A \mapsto A^T$$

(where A^T, as usual, denotes the transpose of a matrix A) is a ring isomorphism.

[**Hint:** In **(a)**, you only have to check the ring axioms that have to do with multiplication. Similarly, in **(b)**, you are free to check the one axiom relating to multiplication only. In **(c)**, you can use [Grinbe19, Exercise 6.5] without proof.]

1.1 Remark

This exercise gives some examples of rings $\mathbb{K}$ that are isomorphic to their opposite rings $\mathbb{K}^{\mathrm{op}}$. See `https://mathoverflow.net/questions/64370/` for examples of rings that are not.

1.2 Solution

[...]

---

2 Exercise 2: More ring isomorphisms

2.1 Problem

(a) Let $\mathbb{L}$ be a ring. Let $w \in \mathbb{L}$ be an invertible element. Prove that the map

$$\mathbb{L} \to \mathbb{L}, \qquad a \mapsto waw^{-1}$$

is a ring isomorphism.

(b) Let $\mathbb{K}$ be a ring. Let W be the $n \times n$-matrix

$$([i+j=n+1])_{1\le i\le n,\ 1\le j\le n} = \begin{pmatrix} 0 & \cdots & 0 & 0 & 1 \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 1 & 0 & 0 \\ \vdots & \iddots & \vdots & \vdots & \vdots \\ 1 & \cdots & 0 & 0 & 0 \end{pmatrix} \in \mathbb{K}^{n\times n}$$

(where we are using the Iverson bracket notation again).

Prove that $W = W^{-1}$.

(c) Let $A = (a_{i,j})_{1\le i\le n,\ 1\le j\le n} \in \mathbb{K}^{n\times n}$ be any $n \times n$-matrix. Prove that

$$WAW^{-1} = (a_{n+1-i,n+1-j})_{1\le i\le n,\ 1\le j\le n}\,.$$

(In other words, WAW^{-1} is the $n \times n$-matrix obtained from A by reversing the order of the rows and also reversing the order of the columns.)

2.2 Remark

The map

$$\mathbb{L} \to \mathbb{L}, \qquad a \mapsto waw^{-1}$$

in part **(a)** of this exercise is called *conjugation by* w. It is best known in the case of a matrix ring, where it corresponds to a change of basis for an endomorphism of a vector space. When $\mathbb{K}$ is a field, the **only** ring isomorphisms $\mathbb{K}^{n\times n} \to \mathbb{K}^{n\times n}$ are conjugations by invertible matrices; this is the Noether–Skolem theorem (in one of its less general variants).

2.3 Solution

[...]

---

3 Exercise 3: Entangled inverses

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

A *left inverse* of an element $x \in \mathbb{K}$ is defined to be a $y \in \mathbb{K}$ such that $yx = 1$.

A *right inverse* of an element $x \in \mathbb{K}$ is defined to be a $y \in \mathbb{K}$ such that $xy = 1$.

Let a and b be two elements of $\mathbb{K}$. Prove the following:

(a) If c is a left inverse of $1 - ab$, then $1 + bca$ is a left inverse of $1 - ba$.

(b) If c is a right inverse of $1 - ab$, then $1 + bca$ is a right inverse of $1 - ba$.

(c) If c is an inverse of $1 - ab$, then $1 + bca$ is an inverse of $1 - ba$.

Here and in the following, the word "*inverse*" (unless qualified with an adjective) means "multiplicative inverse".

3.1 Solution

[...]

---

4 Exercise 4: Composition of ring homomorphisms

4.1 Problem

Let $\mathbb{K}$, $\mathbb{L}$ and $\mathbb{M}$ be three rings. Prove the following:

(a) If $f : \mathbb{K} \to \mathbb{L}$ and $g : \mathbb{L} \to \mathbb{M}$ are two ring homomorphisms, then $g \circ f : \mathbb{K} \to \mathbb{M}$ is a ring homomorphism.

(b) If $f : \mathbb{K} \to \mathbb{L}$ and $g : \mathbb{L} \to \mathbb{M}$ are two ring isomorphisms, then $g \circ f : \mathbb{K} \to \mathbb{M}$ is a ring isomorphism.

4.2 Solution

[...]

---

5 Exercise 5: Squares in finite fields I

5.1 Problem

Let $\mathbb{F}$ be a field.

(a) Prove that if $a, b \in \mathbb{F}$ satisfy $ab = 0$, then $a = 0$ or $b = 0$.

(b) Prove that if $a, b \in \mathbb{F}$ satisfy $a^2 = b^2$, then $a = b$ or $a = -b$.

Recall that an element $\eta \in \mathbb{F}$ is called a *square* if there exists some $\alpha \in \mathbb{F}$ such that $\eta = \alpha^2$.

From now on, assume that $2 \cdot 1_{\mathbb{F}} \neq 0_{\mathbb{F}}$ (that is, $1_{\mathbb{F}} + 1_{\mathbb{F}} \neq 0_{\mathbb{F}}$). Note that this is satisfied whenever $\mathbb{F} = \mathbb{Z}/p$ for a prime $p > 2$ (but also for various other finite fields), but fails when $\mathbb{F} = \mathbb{Z}/2$.

(c) Prove that $a \neq -a$ for every nonzero $a \in \mathbb{F}$.

From now on, assume that $\mathbb{F}$ is finite.

(d) Prove that the number of squares in $\mathbb{F}$ is $\dfrac{1}{2}(|\mathbb{F}| + 1)$.

(e) Conclude that $|\mathbb{F}|$ is odd.

[**Hint:** For part **(d)**, argue that each nonzero square in $\mathbb{F}$ can be written as α^2 for exactly two $\alpha \in \mathbb{F}$.]

5.2 Solution

[...]

---

6 Exercise 6: The characteristic of a field

6.1 Problem

Let $\mathbb{F}$ be a field. Recall that we have defined na to mean $\underbrace{a + a + \cdots + a}_{n \text{ times}}$ whenever $n \in \mathbb{N}$ and $a \in \mathbb{F}$.

Assume that there exists a positive integer n such that $n \cdot 1_{\mathbb{F}} = 0$. Let p be the **smallest** such n.

Prove that p is prime.

[**Hint:** $(a \cdot 1_{\mathbb{F}}) \cdot (b \cdot 1_{\mathbb{F}}) = ab \cdot 1_{\mathbb{F}}$ for all $a, b \in \mathbb{N}$.]

6.2 Remark

The p we just defined is called the *characteristic* of the field $\mathbb{F}$ when it exists. (Otherwise, the characteristic of the field $\mathbb{F}$ is defined to be 0.)

Thus, for each prime p, the finite field $\mathbb{Z}/p$, as well as the finite field of size p^2 that we constructed in class, have characteristic p.

6.3 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` .