Drexel University, Department of Mathematics

Math 533: Abstract Algebra I, Winter 2021: Homework 1

Please solve **at most 5 of the 10 problems!***

Darij Grinberg

February 7, 2021

1 Exercise 1

1.1 Problem

Fix an integer m. An *m-integer* shall mean a rational number r such that there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$.

For example:

- Each integer r is an m-integer (since $m^k r \in \mathbb{Z}$ for $k = 0$).
- The rational number $\dfrac{5}{12}$ is a 6-integer (since $6^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ for $k = 2$), but neither a 2-integer nor a 3-integer (since multiplying it by a power of 2 will not "get rid of" the

*I recommend solving as many problems as you can and wish, but I will only grade and score 5 solutions per submission (and if you submit more, I get to pick which ones I grade).
Results stated in class, and claims of previous problems (even if you did not solve these previous problems), can be used without proof. For example, in solving Problem 5, you can use the result of Problem 2 without proof.
I expect approximately the level of detail that I give in class. Purely straightforward arguments (like checking the ring axioms for a direct product of rings) need not be spelled out; I only expect a note of their necessity.

prime factor 3 in the denominator, and vice versa[1]).

- The 1-integers are the integers (since $1^k r = r$ for all r).
- Every rational number r is a 0-integer (since $0^k r \in \mathbb{Z}$ for $k = 1$).

Let R_m denote the set of all m-integers. Prove that R_m is a subring of $\mathbb{Q}$.

1.2 Remark

The ring R_m is an example of a ring "between $\mathbb{Z}$ and $\mathbb{Q}$" (in the sense that $\mathbb{Z}$ is a subring of R_m, while R_m is a subring of $\mathbb{Q}$). Note that $R_1 = \mathbb{Z}$ and $R_0 = \mathbb{Q}$, whereas $R_2 = R_4 = R_8 = \cdots$ is the ring of all rational numbers that can be written in the form $a/2^k$ with $a \in \mathbb{Z}$ and $k \in \mathbb{N}$.

1.3 Solution

...

---

2 Exercise 2

2.1 Problem

Let R be a ring.

An element a of R is said to be *idempotent* if it satisfies $a^2 = a$.

An element a of R is said to be *involutive* if it satisfies $a^2 = 1$.

(a) Let $a \in R$. Prove that if a is idempotent, then $1 - 2a$ is involutive.

(b) Now, assume that 2 is *cancellable* in R; this means that if u and v are two elements of R satisfying $2u = 2v$, then $u = v$. Prove that the converse of the claim of part **(a)** holds: If $a \in R$ is such that $1 - 2a$ is involutive, then a is idempotent.

(c) Now, let $R = \mathbb{Z}/4\mathbb{Z}$. Find an element $a \in R$ such that $1 - 2a$ is involutive, but a is not idempotent.

2.2 Remark

The idempotent elements of $\mathbb{R}$ are 0 and 1. The involutive elements of $\mathbb{R}$ are 1 and -1. A matrix ring like $\mathbb{R}^{n \times n}$ usually has infinitely many idempotent elements (viz., all projection matrices on subspaces of $\mathbb{R}^n$) and infinitely many involutive elements (viz., all matrices A satisfying $A^2 = I_n$; for instance, all reflections across hyperplanes are represented by such matrices).

Part **(a)** of this exercise assigns an involutive element to each idempotent element of R. If 2 is invertible in R (that is, if the element $2 \cdot 1_R$ has a multiplicative inverse), then this

[1] To make this more rigorous: If we had $2^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ for some $k \in \mathbb{N}$, then we would have $12 \mid 2^k \cdot 5$, which would entail that $3 \mid 12 \mid 2^k \cdot 5$, and thus 3 would appear as a factor in the prime factorization of $2^k \cdot 5$. But this is absurd. Hence, $2^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ cannot hold. Similarly, $3^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ cannot hold.

assignment is a bijection (as can be easily derived from part **(b)**). Note that this assignment, when applied to a matrix ring $\mathbb{R}^{n\times n}$, is exactly the assignment you would expect from the geometric point of view: To the orthogonal projection on a hyperplane H, it assigns the reflection in the hyperplane H. Part **(c)** shows that we cannot drop the "2 is cancellable" condition in part **(b)**.

2.3 Solution

...

---

3 Exercise 3

3.1 Problem

In this exercise, we shall see how idempotent elements are responsible for rings decomposing as direct products.

Let R be a ring, and let e be an idempotent element of R.

(a) Show that $1-e \in R$ is again idempotent.

Now, assume that R is commutative.

(b) Show that the principal ideal eR is itself a ring, with addition and multiplication inherited from R and with zero 0_R and with unity e. (This makes eR a subring of R in the sense of [DF], but not in our sense, since its unity is not generally the unity of R.)

(c) Show that the same holds for the principal ideal $(1-e)\,R$ (except that its unity will be $1-e$ instead of e).

(d) Consider the map

$$\begin{aligned} f : (eR) \times ((1-e)\,R) &\to R, \\ (a, b) &\mapsto a+b. \end{aligned}$$

Prove that this map f is a ring isomorphism.

3.2 Remark

Part **(d)** of this exercise shows that if a commutative ring R has an idempotent element e, then R can be decomposed (up to isomorphism) as a direct product $A \times B$ of two rings A and B (namely, $A = eR$ and $B = (1-e)\,R$). If e is not one of the two trivial idempotents 0 and 1, then these two rings A and B will be nontrivial, so the decomposition really deserves its name.[2]

[2] As an example, take $R = \mathbb{Z}/6\mathbb{Z}$, and let e be the idempotent element $\overline{3} = 3 + 6\mathbb{Z}$ of R (this is idempotent since $3^2 = 9 \equiv 3 \mod 6$ and thus $\overline{3}^2 = \overline{3^2} = \overline{3}$). Then, $eR = \left\{\overline{0}, \overline{3}\right\} \cong \mathbb{Z}/2\mathbb{Z}$ and $(1-e)\,R = \left\{\overline{0}, \overline{2}, \overline{4}\right\} \cong \mathbb{Z}/3\mathbb{Z}$. Hence, the ring isomorphism $R \cong (eR) \times ((1-e)\,R)$ becomes the ring isomorphism $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ that we have seen in class (as an instance of the Chinese Remainder Theorem).

Conversely, any direct product of two nontrivial rings has nontrivial idempotents: If R and S are two rings, then $(1_R, 0_S)$ and $(0_R, 1_S)$ are two idempotent elements of the direct product $R \times S$.

Parts **(b)**, **(c)** and **(d)** of the exercise can be generalized somewhat: Instead of requiring R to be commutative, it suffices to require that $er = re$ for all $r \in R$. We cannot, however, drop this requirement altogether (otherwise, matrix rings would decompose as direct products – as they have lots of idempotent elements –, but typically they don't).

3.3 Solution

...

---

4 Exercise 4

4.1 Problem

In set theory, the *symmetric difference* of two sets A and B is defined to be the set $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$. This symmetric difference is denoted by $A \triangle B$.

Now, let S be any set. Let $\mathcal{P}(S)$ denote the power set of S (that is, the set of all subsets of S). It is easy to check that the following ten properties hold:

$$\begin{aligned}
A \triangle B &= B \triangle A && \text{for any sets } A \text{ and } B;\\
A \cap B &= B \cap A && \text{for any sets } A \text{ and } B;\\
(A \triangle B) \triangle C &= A \triangle (B \triangle C) && \text{for any sets } A, B \text{ and } C;\\
(A \cap B) \cap C &= A \cap (B \cap C) && \text{for any sets } A, B \text{ and } C;\\
A \triangle \varnothing &= \varnothing \triangle A = A && \text{for any set } A;\\
A \triangle A &= \varnothing && \text{for any set } A;\\
A \cap S &= S \cap A = A && \text{for any subset } A \text{ of } S;\\
\varnothing \cap A &= A \cap \varnothing = \varnothing && \text{for any set } A;\\
A \cap (B \triangle C) &= (A \cap B) \triangle (A \cap C) && \text{for any sets } A, B \text{ and } C;\\
(A \triangle B) \cap C &= (A \cap C) \triangle (B \cap C) && \text{for any sets } A, B \text{ and } C.
\end{aligned}$$

Therefore, $\mathcal{P}(S)$ becomes a commutative ring, where the addition is defined to be the operation $\triangle$, the multiplication is defined to be the operation $\cap$, the zero is defined to be the set $\varnothing$, and the unity is defined to be the set S. (The ten properties listed above show that the axioms of a commutative ring are satisfied for $(\mathcal{P}(S), \triangle, \cap, \varnothing, S)$. In particular, the sixth property shows that every subset A of S has an additive inverse – namely, itself. Of course, it is unusual for an element of a commutative ring to be its own additive inverse, but in this example it happens all the time!)

The commutative ring $\mathcal{P}(S)$ has the property that $a \cdot a = a$ for every $a \in \mathcal{P}(S)$. (This simply means that $A \cap A = A$ for every $A \subseteq S$.) Rings that have this property are called *Boolean rings*. (Of course, $\mathcal{P}(S)$ is the eponymic example for a Boolean ring; but there are also others.)

(a) Prove that the ring $\mathcal{P}(S)$ is isomorphic to the direct product $(\mathbb{Z}/2\mathbb{Z})^S = \prod_{s \in S} (\mathbb{Z}/2\mathbb{Z})$.

(b) Let F be the set of all **finite** subsets of S. Prove that F is an ideal of $\mathcal{P}(S)$.

(c) Assume that S is infinite. Prove that the ideal F is not principal.

(d) Instead, assume that S is finite. Prove that every ideal of $\mathcal{P}(S)$ is principal.

[**Hint:** For part **(d)**, let I be an ideal of $\mathcal{P}(S)$, and pick a subset $T \in I$ of largest size. Argue that each subset of T must also belong to I. Conclude that every set in I must be a subset of T.]

4.2 Solution

...

---

5 Exercise 5

5.1 Problem

Now we shall study Boolean rings in general.

A *Boolean ring* means a ring R such that every $a \in R$ satisfies $a^2 = a$ (that is, every $a \in R$ is idempotent). (Keep in mind that rings must have a 1 according to our definition.)

Let R be a Boolean ring. Prove the following:

(a) We have $2a = 0$ for each $a \in R$.

(b) We have $-a = a$ for each $a \in R$.

(c) The ring R is commutative.

(d) If R is finite, then $R \cong (\mathbb{Z}/2\mathbb{Z})^n$ for some $n \in \mathbb{N}$.

[**Hint:** In part **(a)**, use $a^2 = a$ and $(a+1)^2 = a+1$. In part **(c)**, expand $(a+b)^2$ (but don't use the binomial formula, since you don't know yet that $ab = ba$). Finally, for part **(d)**, use strong induction on $|R|$ as follows: Pick some $e \in R$ that is distinct from 0 and 1 (if no such e exists, the claim is obvious). Then, e is idempotent, so Exercise 3 **(d)** decomposes the ring R as a direct product of two smaller rings. You can use without proof that direct products are associative up to isomorphism (so that $A_1 \times A_2 \times \cdots \times A_m \cong (A_1 \times A_2 \times \cdots \times A_k) \times (A_{k+1} \times A_{k+2} \times \cdots \times A_m)$ for any rings $A_1, A_2, \ldots, A_m$).]

5.2 Solution

...

---

6 Exercise 6

6.1 Problem

Let A be the 2×2-matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ over $\mathbb{Z}$. Consider also the identity matrix $I_2 \in \mathbb{Z}^{2\times 2}$.

Let $\mathcal{F}$ be the subset

$$\{aA + bI_2 \mid a, b \in \mathbb{Z}\} = \left\{ \begin{pmatrix} b & a \\ a & a+b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

of the matrix ring $\mathbb{Z}^{2\times 2}$.

(a) Prove that $A^2 = A + I_2$.

(b) Prove that the set $\mathcal{F}$ is a **commutative** subring of $\mathbb{Z}^{2\times 2}$.

Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence. This is the sequence of integers defined recursively by

$$f_0 = 0, \qquad f_1 = 1, \qquad \text{and} \qquad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 2.$$

The first entries of this sequence are

n	0	1	2	3	4	5	6	7	8	9	10	11	12
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144

.

(c) Prove that $A^n = f_n A + f_{n-1} I_2$ for all positive integers n.

(d) Prove that $f_{n+m} = f_n f_{m+1} + f_{n-1} f_m$ for all positive integers n and all $m \in \mathbb{N}$.

Now, define a further matrix $B \in \mathcal{F}$ by $B = (-1)\, A + 1 I_2 = I_2 - A$.

(e) Prove that $B^2 = B + I_2$ and $B^n = f_n B + f_{n-1} I_2$ for all positive integers n.

(f) Prove that $A^n - B^n = f_n\,(A - B)$ for all $n \in \mathbb{N}$.

(g) Prove that $f_d \mid f_{dn}$ for any nonnegative integers d and n.

[**Hint:** In part **(b)**, don't forget to check commutativity! It is not inherited from $\mathbb{Z}^{2\times 2}$, since $\mathbb{Z}^{2\times 2}$ is not commutative.

One way to prove **(d)** is by comparing the $(1,1)$-th entries of the two (equal) matrices $A^n A^{m+1}$ and A^{n+m+1}, after first using part **(c)** to expand these matrices.

For part **(g)**, compare the $(1,1)$-th entries of the matrices $A^d - B^d$ and $A^{dn} - B^{dn}$, after first proving that $A^d - B^d \mid A^{dn} - B^{dn}$ in the commutative ring $\mathcal{F}$. Note that divisibility is a tricky concept in general rings, but $\mathcal{F}$ is a commutative ring, which lets many arguments from the integer setting go through unchanged.]

6.2 Solution

...

7 Exercise 7

7.1 Problem

Let R be a ring. An element $a \in R$ is said to be *nilpotent* if there exists an $n \in \mathbb{N}$ such that $a^n = 0$. (For example, the residue class $\overline{6}$ in $\mathbb{Z}/8\mathbb{Z}$ is nilpotent, since its 3-rd power is $\overline{0}$.)

(a) If a and b are two nilpotent elements of R satisfying $ab = ba$, then prove that $a + b$ is nilpotent as well.

(b) Find a counterexample to part **(a)** if we don't assume $ab = ba$.

(c) Assume that the ring R is commutative. Let N be the set of all nilpotent elements of R. Prove that N is an ideal of R.

7.2 Remark

The ideal N in part **(c)** of this exercise is known as the *nilradical* of R.

7.3 Solution

...

---

8 Exercise 8

8.1 Problem

Let R be a ring. Prove the following:

(a) Let I and J be two ideals of a ring R. Then, $I + J$ and $I \cap J$ and IJ are ideals of R as well.

(b) Let I and J be two ideals of a ring R. Then, $IJ \subseteq I \cap J \subseteq I \subseteq I + J$ and $IJ \subseteq I \cap J \subseteq J \subseteq I + J$.

(c) The set of all ideals of R is a monoid with respect to the binary operation $+$, with neutral element $\{0_R\} = 0R$. That is,

$$(I + J) + K = I + (J + K) \qquad \text{for any three ideals } I, J, K \text{ of } R;$$
$$I + \{0_R\} = \{0_R\} + I = I \qquad \text{for any ideal } I \text{ of } R.$$

(d) The set of all ideals of R is a monoid with respect to the binary operation $\cdot$, with neutral element $R = 1R$. That is,

$$(IJ)\,K = I\,(JK) \qquad \text{for any three ideals } I, J, K \text{ of } R;$$
$$IR = RI = I \qquad \text{for any ideal } I \text{ of } R.$$

[**Hint:** You can be terse here, as there is a lot to show, much of it straightforward. I recommend using the notion of "(I, J)-products" from lecture 4; it is often easier to talk abstractly about sums of (I, J)-products than to write them out as $i_1 j_1 + i_2 j_2 + \cdots + i_k j_k$. For the proof of $(IJ)\,K = I\,(JK)$, I recommend first showing that any (IJ, K)-product belongs to $I\,(JK)$.]

8.2 Solution

...

---

9 Exercise 9

9.1 Problem

Let R be a ring. Let a and b be two elements of R. Prove the following: If c is an inverse of $1-ab$, then $1+bca$ is an inverse of $1-ba$.

9.2 Remark

This yields a well-known result in functional analysis; see `https://math.stackexchange.com/questions/79217` .

9.3 Solution

...

---

10 Exercise 10

10.1 Problem

Let F be a field.

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

An element $\eta \in F$ is called a *square* if there exists some $\alpha \in F$ such that $\eta = \alpha^2$. For example, the squares in $\mathbb{Z}/7\mathbb{Z}$ are the four elements $\overline{0}, \overline{1}, \overline{2}, \overline{4}$. (Indeed, this is equivalent to the answer to Exercise 7 **(a)** on homework set #0.)

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

(b) Prove that $a \neq -a$ for every nonzero $a \in F$.

From now on, assume that F is finite.

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

(d) Conclude that $|F|$ is odd.

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

10.2 Solution

...

References

[DF] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.