Drexel University, Department of Mathematics

Math 533: Abstract Algebra I, Winter 2021: Homework 2

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

Darij Grinberg

February 28, 2021

1 Exercise 1

1.1 Problem

Let R be a ring. Let a be a nilpotent element of R. (Recall that "nilpotent" means that there exists some $n \in \mathbb{N}$ such that $a^n = 0$.)

(a) Prove that $1 - a \in R$ is a unit.

(b) Let $u \in R$ be a unit satisfying $ua = au$. Prove that $u - a \in R$ is a unit.

[**Hint:** Treat the geometric series $\dfrac{1}{1-x} = 1 + x + x^2 + \cdots$ as an inspiration. Nilpotent elements of a ring are an algebraic analogue of the infamous "sufficiently small $\varepsilon > 0$" from real analysis. In particular, a nilpotent element a can be substituted (for x) into any formal power series $r_0 + r_1 x + r_2 x^2 + \cdots$, since the resulting sum will have only finitely many addends distinct from 0. (You don't actually need to write any infinite sums in your solution, but they can help you come up with the solution in the first place.)]

1.2 Solution

...

2 Exercise 2

2.1 Problem

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

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

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

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

This new ring is called the *opposite ring* of R, and is denoted by R^{op}.

Note that the **sets** R and R^{op} are identical (so a map from R to R is the same as a map from R to R^{op}); but the **rings** R and R^{op} are generally not the same (so a ring morphism from R to R is not the same as a ring morphism from R to R^{op}).

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

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

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

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

(d) Forget about S, and let R be an arbitrary ring again. Let M be a right R-module. Prove that M becomes a left R^{op}-module if we define an action of R^{op} on M by

$$rm = mr \qquad \text{for all } r \in R^{\mathrm{op}} \text{ and } m \in M.$$

(Here, the left hand side is to be understood as the image of (r, m) under the new action of R^{op} on M, whereas the right hand side is the image of (m, r) under the original action of R on M.)

[**Hint:** There are many straightforward axioms to check. Don't give too many details; one sentence per axiom should suffice (e.g., in part **(d)**, you can say "left distributivity for the left R^{op}-module M follows from right distributivity from the right R-module M", or even "the distributivity axioms for the new module boil down to the distributivity axioms for the old module"). In parts **(a)**, **(b)** and **(d)**, you only have to check the axioms that have to do with multiplication. In **(c)**, you can use basic properties of transposes of matrices without proof, as long as you say clearly which properties you are using. You will need to use the commutativity of S in one place.]

2.2 Remark

Parts **(b)** and **(c)** of this exercise gives some examples of rings R that are isomorphic to their opposite rings R^{op}. See `https://mathoverflow.net/questions/64370/` for examples of rings that are not.

2.3 Solution

...

3 Exercise 3

3.1 Problem

Let R be an integral domain. Let $a \in R$ and $b \in R$. Assume that a and b have an lcm $\ell \in R$. Prove that a and b have a gcd $g \in R$, which furthermore satisfies $g\ell = ab$.

[**Hint:** If u and v are two elements of an integral domain R, with $v \neq 0$, then you can use the notation $\dfrac{u}{v}$ (or u/v) for the element $w \in R$ satisfying $u = vw$. This element w does not always exist, but when it does, it is unique, so the notation is unambiguous. It is also easy to see that standard rules for fractions, such as $\dfrac{u}{v} + \dfrac{x}{y} = \dfrac{uy + vx}{vy}$ and $\dfrac{u}{v} \cdot \dfrac{x}{y} = \dfrac{ux}{vy}$, hold as long as the fractions $\dfrac{u}{v}$ and $\dfrac{x}{y}$ exist.]

3.2 Remark

The converse is not true: The existence of a gcd does not imply the existence of an lcm.

3.3 Solution

...

4 Exercise 4

4.1 Problem

Let p be a prime number.

- **(a)** Prove that if a and b are two integers such that $a^2 \equiv b^2 \mod p^2$, then $a \equiv b \mod p^2$ or $a \equiv -b \mod p^2$ or $a \equiv b \equiv 0 \mod p$.
- **(b)** Compute the number of squares in the ring $\mathbb{Z}/p^2$.

4.2 Remark

This is one more step on our quest to count the squares in $\mathbb{Z}/n$ for an arbitrary positive integer n.

4.3 Solution

...

---

5 Exercise 5

5.1 Problem

Let p be a prime number.

(a) Prove that the only units of the ring $\mathbb{Z}/p$ that are their own inverses (i.e., the only $m \in (\mathbb{Z}/p)^{\times}$ that satisfy $m^{-1} = m$) are $\overline{1}$ and $\overline{-1}$.

(b) Assume that p is odd. Let $u = \dfrac{p-1}{2} \in \mathbb{N}$. Prove that $u!^2 \equiv -(-1)^u \mod p$.

[**Hint:** The two parts of the exercise are unrelated, other than both being lemmas in our Lecture 7. For part **(b)**, recall Wilson's theorem.]

5.2 Remark

Part **(b)** of this exercise easily yields that $u!^2 \equiv -1 \mod p$ if $p \equiv 1 \mod 4$ (since $p \equiv 1 \mod 4$ entails that u is even). This is one of the facts we used in Lecture 7.]

5.3 Solution

...

---

6 Exercise 6

6.1 Problem

Recall the ring $\mathbb{Z}[i]$ of Gaussian integers. Let $N : \mathbb{Z}[i] \to \mathbb{N}$ be the map that sends each Gaussian integer $z = a + bi \in \mathbb{Z}[i]$ (with $a, b \in \mathbb{Z}$) to $a^2 + b^2 = |z|^2$. (This is the Euclidean norm on $\mathbb{Z}[i]$ that we have already used several times.)

(a) Prove that if z and w are two Gaussian integers satisfying $z \mid w$ in $\mathbb{Z}[i]$, then $N(z) \mid N(w)$ in $\mathbb{Z}$.

(b) Let $z = a + bi \in \mathbb{Z}[i]$ with $a, b \in \mathbb{Z}$. Assume that $z \neq 0$. Let $n = \lfloor |z| \rfloor = \left\lfloor \sqrt{a^2 + b^2} \right\rfloor$. Prove that every divisor of z in $\mathbb{Z}[i]$ has the form $c + di$ with $c, d \in \{-n, -n+1, \ldots, n\}$.

(c) Without recourse to the general theory of PIDs and UFDs, prove that every nonzero element of $\mathbb{Z}[i]$ has an irreducible factorization.

(d) Let $z \in \mathbb{Z}[i]$. Prove that we have the following logical equivalence:

$$(z \text{ is a unit of } \mathbb{Z}[i]) \iff (N(z) = 1) \iff (z \in \{1, i, -1, -i\}).$$

6.2 Remark

Combining parts **(b)** and **(c)** of this exercise yields a (slow) algorithm for finding an irreducible factorization of a nonzero Gaussian integer. (Indeed, part **(b)** shows that we can list all divisors of a nonzero Gaussian integer in finite time. This allows checking whether a Gaussian integer is prime, and otherwise finding a prime divisor.)

6.3 Solution

...

7 Exercise 7

7.1 Problem

Consider the ring

$$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\right\}.$$

This ring is a subring of $\mathbb{C}$, and thus is an integral domain.

Let $u = 2 \in \mathbb{Z}\left[\sqrt{-3}\right]$ and $v = 1 + \sqrt{-3} \in \mathbb{Z}\left[\sqrt{-3}\right]$. Further let $a = 2u = 4$ and $b = 2v$.

(a) Prove that both u and v are common divisors of a and b in $\mathbb{Z}\left[\sqrt{-3}\right]$.

(b) Prove that the only divisors of 4 in $\mathbb{Z}\left[\sqrt{-3}\right]$ are ± 1, ± 2, ± 4, $\pm\left(1 + \sqrt{-3}\right)$, and $\pm\left(1 - \sqrt{-3}\right)$.

(c) Prove that a and b have no gcd in $\mathbb{Z}\left[\sqrt{-3}\right]$.

[**Hint:** For full credits on part **(b)**, it suffices to explain how the solution can be reduced to a finite computation and perform one representative case of the computation.]

7.2 Remark

This shows that $\mathbb{Z}\left[\sqrt{-3}\right]$ is not a UFD.

7.3 Solution

...

8 Exercise 8

8.1 Problem

Let R be a ring. Let I and J be two ideals of R such that $I \subseteq J$. Let J/I denote the set of all cosets $j + I \in R/I$ where $j \in J$.

Prove the following:

(a) This set J/I is an ideal of R/I.

(b) We have $(R/I) / (J/I) \cong R/J$ (as rings). More concretely, there is a ring isomorphism $R/J \to (R/I) / (J/I)$ that sends each residue class $\overline{r} = r+J$ to $\overline{r+I} = (r+I)+(J/I)$.

8.2 Remark

This is known as the *Third Isomorphism Theorem for rings.*

For an example, take $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$ and $J = 2\mathbb{Z}$. In this case, J/I consists of the "even" residue classes $\overline{0}, \overline{2}, \overline{4}$ in $R/I = \mathbb{Z}/6$. Part **(b)** of the exercise says that if we "quotient them out" of $\mathbb{Z}/6$, then we are left with (an isomorphic copy of) $R/J = \mathbb{Z}/2$.

8.3 Solution

...

9 Exercise 9

9.1 Problem

Let R be a ring. Let S be a subring of R. Let I be an ideal of R. Define $S + I$ to be the subset $\{s + i \mid s \in S \text{ and } i \in I\}$ of R.

Prove the following:

(a) This subset $S + I$ is a subring of R.

(b) The set I is an ideal of the ring $S + I$.

(c) The set $S \cap I$ is an ideal of the ring S.

(d) We have $(S + I) / I \cong S / (S \cap I)$ (as rings). More concretely, there is a ring isomorphism $S / (S \cap I) \to (S + I) / I$ that sends each residue class $\overline{s} = s + (S \cap I)$ to $\overline{s} = s + I$.

9.2 Remark

This is known as the *Second Isomorphism Theorem for rings.*

For an example, we can let

- R be the polynomial ring $\mathbb{Q}[x]$ of all univariate polynomials with rational coefficients;

- $I = \{a_2 x^2 + a_3 x^3 + \cdots + a_n x^n \mid n \geq 0 \text{ and } a_i \in \mathbb{Q}\}$ be the ideal consisting of all polynomials divisible by x^2 (that is, all polynomials whose x^0-coefficient and x^1-coefficient are 0);
- S be the subring $\mathbb{Q}$ of R (which consists of all constant polynomials).

Then, $S + I = \{a_0 + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n \mid n \geq 0 \text{ and } a_i \in \mathbb{Q}\}$ is the set of all polynomials whose x^1-coefficient is 0. This is indeed a subring of R, as we have seen in Lecture 6 (where we have used this subring to find an irreducible element that is not prime).

9.3 Solution

...

10 Exercise 10

10.1 Problem

(a) Let R be a commutative ring, and let u and n be two nonnegative integers. Let $x, y \in R$ be two elements such that $x - y \in uR$. (Here, $uR := \{ur \mid r \in R\}$; this is a principal ideal of R, since $uR = (u1_R) R$.)

Prove that
$$x^n - y^n \in guR, \qquad \text{where } g = \gcd(n, u).$$

(b) Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence, defined as in Exercise 6 on homework set #1. Prove that
$$\gcd(n, f_d) \cdot f_d \mid f_{dn} \qquad \text{for any } d, n \in \mathbb{N}.$$

[**Hint:** For part **(a)**, write $x^n - y^n$ as $(x - y)(x^{n-1} + x^{n-2} y + \cdots + y^{n-1})$, and show that the second factor belongs to gR. For part **(b)**, define the matrices A and B and the commutative ring $\mathcal{F}$ as in Exercise 6 on homework set #1, and apply part **(a)** to $x = A^d$ and $y = B^d$ and $u = f_d$.]

10.2 Solution

...

References