Drexel University, Department of Mathematics

Math 533: Abstract Algebra I, Winter 2021: Homework 3

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

Darij Grinberg

February 12, 2023

1 Exercise 1

1.1 Problem

Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Prove the following:

(a) If K is an ideal of S, then $f^{-1}(K) := \{r \in R \mid f(r) \in K\}$ is an ideal of R that satisfies $\operatorname{Ker} f \subseteq f^{-1}(K)$.

Now, assume that f is surjective. Prove the following:

(b) If J is an ideal of R, then $f(J) := \{f(j) \mid j \in J\}$ is an ideal of S.

(c) The maps

$$\{\text{ideals } J \text{ of } R \text{ satisfying } \operatorname{Ker} f \subseteq J\} \to \{\text{ideals of } S\}, \quad J \mapsto f(J)$$

and

$$\{\text{ideals of } S\} \to \{\text{ideals } J \text{ of } R \text{ satisfying } \operatorname{Ker} f \subseteq J\}, \quad K \mapsto f^{-1}(K)$$

are mutually inverse.

1.2 Remark

It is easy to find a counterexample to the claim of part **(b)** if the "f is surjective" assumption is dropped.

Part **(c)** is one form of the "Fourth Isomorphism Theorem for Rings". Indeed, let R be a ring, and let I be an ideal of R. Then, the canonical projection $\pi : R \to R/I$ is a surjective ring morphism whose kernel $\operatorname{Ker} \pi$ is I. Thus, applying part **(c)** to $S = R/I$ and $f = \pi$, we see that the maps

$$\{\text{ideals } J \text{ of } R \text{ satisfying } I \subseteq J\} \to \{\text{ideals of } R/I\}, \\ J \mapsto \pi(J) = J/I$$

and

$$\{\text{ideals of } R/I\} \to \{\text{ideals } J \text{ of } R \text{ satisfying } I \subseteq J\}, \\ K \mapsto \pi^{-1}(K) = \{r \in R \mid r + I \in K\}$$

are mutually inverse. (Here, J/I is defined as in Exercise 8 on homework set #2.)

1.3 Solution

...

---

2 Exercise 2

2.1 Problem

Let R be a commutative ring. Let I be an ideal of R.

- The ideal I is said to be *proper* if it is a proper subset of R (that is, $I \neq R$).
- The ideal I is said to be *prime* if it is proper and has the following property: If $a, b \in R$ satisfy $ab \in I$, then $a \in I$ or $b \in I$.
- The ideal I is said to be *maximal* if it is proper and the only ideals J of R satisfying $I \subseteq J \subseteq R$ are I and R.

Prove the following:

(a) The ideal I is prime if and only if the quotient ring R/I is an integral domain.

(b) The ideal I is maximal if and only if the quotient ring R/I is a field.

(c) Any maximal ideal I of R is prime.

[**Hint:** In part **(b)**, it helps to first classify the nontrivial commutative rings S that have no ideals other than $\{0\}$ and S.]

2.2 Remark

A principal ideal aR of R (with $a \in R$ nonzero) is prime if and only if a is a prime element of R. Thus, the notion of prime ideals generalizes the notion of prime elements (and, ultimately, that of prime numbers).

2.3 Solution

...

---

3 Exercise 3

3.1 Problem

Let A be an abelian group (written additively). Prove that there is at most one map $\mathbb{Q} \times A \to A$ that makes A into a $\mathbb{Q}$-module.

[**Hint:** Let $*_1$ and $*_2$ denote two such maps. Let $r, s \in \mathbb{Z}$ and $a \in A$ with $s \neq 0$. Your goal is to show that $\frac{r}{s} *_1 a = \frac{r}{s} *_2 a$. First prove that if two elements $u, v \in A$ satisfy $s *_1 u = s *_1 v$, then $u = v$.]

3.2 Solution

...

---

4 Exercise 4

4.1 Problem

Prove the *Chinese Remainder Theorem for Modules*:

Let R be a commutative ring. Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of R. Let M be a R-module. Then:[1]

(a) We have[2] $I_1M \cap I_2M \cap \cdots \cap I_kM = I_1I_2 \cdots I_kM$.

(b) There is an R-module isomorphism[3]

$$M/\left(I_1I_2 \cdots I_kM\right) \to (M/I_1M) \times (M/I_2M) \times \cdots \times (M/I_kM)$$

that sends each coset $m+I_1I_2 \cdots I_kM$ to the k-tuple $(m + I_1M, m + I_2M, \ldots, m + I_kM)$.

[1] Keep in mind that if I is an ideal of R, then IM denotes the left R-submodule {finite sums of (I, M)-products} of M (see Lecture 8).

[2] The notation "$I_1M \cap I_2M \cap \cdots \cap I_kM$" means "$(I_1M) \cap (I_2M) \cap \cdots \cap (I_kM)$".

[3] The notation "M/IM" (where I is an ideal of R) means "$M/\left(IM\right)$".

[**Hint:** If some parts of the proof can be done exactly as in the ring case (i.e., as in the proof of the Chinese Remainder Theorem for Rings that we did in class), then you can say so and omit the details; however, you need to be precise about which parts are analogous and which are not.]

4.2 Solution

...

---

5 Exercise 5

5.1 Problem

Let $n \in \mathbb{N}$. Prove that we have $x^2 + x + 1 \mid x^{2n} + x^n + 1$ in the polynomial ring $\mathbb{Z}[x]$ if and only if $3 \nmid n$ in $\mathbb{Z}$.

[**Hint:** First show that $x^3 \equiv 1 \mod x^2 + x + 1$ in the ring $\mathbb{Z}[x]$. Here, we are using the notation $a \equiv b \mod c$ (spoken "a is congruent to b modulo c") for $c \mid a - b$ whenever a, b, c are three elements of a commutative ring R. Congruences in R are a straightforward generalization of congruences of integers (which are known from elementary number theory), and behave just as nicely; in particular, they can be added, subtracted and multiplied.]

5.2 Solution

...

---

6 Exercise 6

6.1 Problem

Let F be a field. Consider the univariate polynomial ring $F[x]$. Let $n \in \mathbb{N}$. Prove the following:

(a) Let $a_1, a_2, \ldots, a_{n+1}$ be $n+1$ distinct elements of F. Let $b_1, b_2, \ldots, b_{n+1}$ be $n+1$ arbitrary elements of F. Then, there is a **unique** polynomial $p \in F[x]$ satisfying $\deg p \leq n$ and

$$p[a_i] = b_i \qquad \text{for all } i \in \{1, 2, \ldots, n+1\}.$$

(b) This polynomial p is given by

$$p = \sum_{j=1}^{n+1} b_j \frac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}$$

(where the "$\prod\limits_{k \neq j}$" sign means a product over all $k \in \{1, 2, \ldots, n+1\}$ satisfying $k \neq j$).

(c) Assume that $F = \mathbb{Q}$. Let $p \in \mathbb{Q}[x]$ be a polynomial of degree $\leq n$ such that

$$p[i] = 2^i \qquad \text{for all } i \in \{0, 1, \ldots, n\}.$$

Find $p[n+1]$.

6.2 Remark

I'm using my notation $p[u]$ for the evaluation $p(u)$, mostly to be on the safe side (I don't think confusion is possible here).

6.3 Solution

...

---

7 Exercise 7

7.1 Problem

Let F be a commutative ring. For each polynomial

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

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

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

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

Let $D : F[x] \to F[x]$ be the map sending each polynomial 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 $f \in F[x]$, then $\deg(f') \leq \deg f - 1$.

(b) The map $D : F[x] \to F[x]$ is F-linear.

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

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

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

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

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

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

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

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

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

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

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

Let $J : F[x] \to F[x]$ be the map sending each polynomial f to its integral $\int f$. Prove the following:

(g) The map $J : F[x] \to F[x]$ is F-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 a and b, and then obtain the general case by interchanging summations.]

7.2 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; 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 a polynomial 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 polynomial f, the polynomial $(J \circ D)(f)$ differs from f only in its constant term.

[4] Just as in class, I am using the notation "$f[u]$" for the evaluation of f at u. The more common notation for this is $f(u)$, but is too easily mistaken for a product.

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

7.3 Solution

...

---

8 Exercise 8

8.1 Problem

Let me define an $\mathbb{R}$-algebra $\mathbb{D}$ that is somewhat analogous to $\mathbb{C}$ (the ring of complex numbers). Namely, I define $\mathbb{D}$ to be the free $\mathbb{R}$-module $\mathbb{R}^2$ (so the elements of $\mathbb{D}$ are pairs of real numbers, and they are added and scaled entrywise), and I define a multiplication on $\mathbb{D}$ by

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

for all $(a,b)\in\mathbb{D}$ and $(c,d)\in\mathbb{D}$. (Compare this with the multiplication of complex numbers, which would have the right hand side $(ac-bd, ad+bc)$ instead.)

(a) Prove that $\mathbb{D}$ thus becomes an $\mathbb{R}$-algebra with zero $(0,0)$ and unity $(1,0)$.

The elements of $\mathbb{D}$ will be called *dual numbers*. We let ε denote the dual number $(0,1)$.

(b) Prove that $a+b\varepsilon = (a,b)$ for any $a,b\in\mathbb{R}$.

(c) Prove that a dual number $\alpha = a+b\varepsilon$ (with $a,b\in\mathbb{R}$) is a unit of $\mathbb{D}$ if and only if $a\neq 0$.

(d) Let $p\in\mathbb{R}[x]$ 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 has been defined in Exercise 7.

(e) Prove that $\mathbb{R}[x]/x^2 \cong \mathbb{D}$ as $\mathbb{R}$-algebras. More concretely: Prove that the map

$$\begin{aligned}\mathbb{R}[x]/x^2 &\to \mathbb{D},\\ \overline{p} &\mapsto p(\varepsilon)\end{aligned}$$

is well-defined and is an $\mathbb{R}$-algebra isomorphism.

8.2 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.

The element $\varepsilon\in\mathbb{D}$ is an example of a nilpotent element in a ring (in a particularly simple way: $\varepsilon^2 = 0$).

The field $\mathbb{R}$ could be replaced by an arbitrary commutative ring R in the above exercise; the only change necessitated by this would be in part **(c)**, where "$\alpha\neq 0$" would have to be replaced by "α is a unit". I have stated the exercise for $\mathbb{R}$ in order to make the analogy to $\mathbb{C}$ more vivid.

8.3 Solution

...

---

9 Exercise 9

9.1 Problem

Let φ be the *golden ratio* – i.e., the real number $\dfrac{1+\sqrt{5}}{2} \approx 1.618\ldots$. Let $\mathbb{Z}[\varphi]$ be the set of all reals of the form $a + b\varphi$ with $a, b \in \mathbb{Z}$.

Consider the ring $\mathcal{F}$ defined in Exercise 6 of homework set #1.

(a) Prove that $\mathbb{Z}[\varphi]$ is a subring of $\mathbb{R}$.

(b) Prove that

$$\mathbb{Z}[\varphi] \cong \mathcal{F} \cong \mathbb{Z}[x] / \left(x^2 - x - 1\right) \qquad \text{as rings.}$$

9.2 Solution

...

---

10 Exercise 10

10.1 Problem

Let R be a ring. Let M and N be two left R-modules. Recall that $\mathrm{Hom}_R(M, N)$ is the set of all left R-module morphisms from M to N.

Prove the following:

(a) The set $\mathrm{Hom}_R(M, N)$ becomes an additive abelian group if we define addition pointwise (i.e., for any $f \in \mathrm{Hom}_R(M, N)$ and $g \in \mathrm{Hom}_R(M, N)$, we define $f + g$ to be the map $M \to N$ that sends each $m \in M$ to $f(m) + g(m)$). Its neutral element is the *zero morphism* $\mathbf{0} : M \to N$ that sends each $m \in M$ to 0. This group $\mathrm{Hom}_R(M, N)$ is called the *Hom group* of M and N.

(b) If R is commutative, then the Hom group $\mathrm{Hom}_R(M, N)$ furthermore becomes an R-module, where the action is defined as follows: For any $r \in R$ and any $f \in \mathrm{Hom}_R(M, N)$, we let $rf \in \mathrm{Hom}_R(M, N)$ be the map that sends each $m \in M$ to $rf(m) \in N$.

(c) If $N = M$, then the Hom group $\mathrm{Hom}_R(M, N) = \mathrm{Hom}_R(M, M)$ becomes a ring if we define multiplication to be composition (i.e., for any for any $f \in \mathrm{Hom}_R(M, M)$ and $g \in \mathrm{Hom}_R(M, M)$, we define fg to be the composition $f \circ g$). Its unity is the identity

map $\mathrm{id} : M \to M$. This ring $\mathrm{Hom}_R(M, M)$ is also denoted $\mathrm{End}_R(M)$ and known as the *endomorphism ring*[6] of M.

(d) If R is commutative and we have $N = M$, then the endomorphism ring $\mathrm{End}_R(M)$ becomes an R-algebra (with the R-module structure defined as in part **(b)**).

(e) Let $M = N = R^{\mathbb{N}}$; this is the left R-module of all infinite sequences $(a_0, a_1, a_2, \ldots)$ of elements of R. Define two left R-module morphisms $f : M \to N$ and $g : M \to N$ by

$$f(a_0, a_1, a_2, \ldots) = (a_1, a_2, a_3, \ldots) \qquad \text{for any } (a_0, a_1, a_2, \ldots) \in M$$

and

$$g(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots) \qquad \text{for any } (a_0, a_1, a_2, \ldots) \in M.$$

Prove that $fg = 1$ but $gf \neq 1$ (unless R is trivial) in the ring $\mathrm{End}_R(M)$.

10.2 Remark

Parts **(a)**–**(d)** are important constructions; endomorphism rings generalize rings of matrices in linear algebra or of operators in functional analysis. Part **(e)** illustrates the difference between inverses and left inverses in a ring. (A *left inverse* of an element a is an element b that satisfies $ba = 1$ but doesn't necessarily satisfy $ab = 1$.)

10.3 Solution

...

References

[6] An *endomorphism* is defined to be a morphism from a structure (e.g., a ring or a module or an algebra) to itself.