Drexel University, Department of Mathematics

Math 533: Abstract Algebra I, Winter 2021: Homework 4

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

Darij Grinberg

February 13, 2023

---

1 Exercise 1

1.1 Problem

Let F be a finite field. Prove the following:

(a) We have $a^{|F|} = a$ for each $a \in F$.

(b) If $i > 1$ is an integer such that each $a \in F$ satisfies $a^i = a$, then $i \geq |F|$.

1.2 Remark

Note that part **(a)** generalizes Fermat's Little Theorem (the part that says that $a^p = a$ for any prime p and any $a \in \mathbb{Z}/p$).

1.3 Solution

...

---

2 Exercise 2

2.1 Problem

Let p be a prime number. Let F be a finite field of characteristic p. Let f be the map $F \to F,\ a \mapsto a^p$. We know (from Lecture 14) that this map f is a ring morphism from F to F (known as the *Frobenius endomorphism* of F).

(a) Prove that f is a ring isomorphism from F to F (so it is invertible).

(b) Now, replace the words "field of characteristic p" by the (more general) "commutative $\mathbb{Z}/p$-algebra" in the above. Find an example where the claim of part **(a)** becomes false.

2.2 Solution

...

---

3 Exercise 3

3.1 Problem

Let S and F be two fields such that S is a subring of F. (For example, we can take $S = \mathbb{Q}$ and $F = \mathbb{R}$.)

For any $a \in F$, we define an *annihilating polynomial of* a to be a polynomial $f \in S[x]$ such that a is a root of f. For instance:

- If $a \in S$, then $x - a$ is an annihilating polynomial of a.
- If a is a square root of an element $v \in S$, then $x^2 - v$ is an annihilating polynomial of a.
- If $S = \mathbb{Q}$ and $F = \mathbb{R}$, then $x^4 - 10x^2 + 1$ is an annihilating polynomial of $\sqrt{2} + \sqrt{3}$.
- The real number π is known to be transcendental; this means that there exists no nonzero annihilating polynomial of π (for $S = \mathbb{Q}$ and $F = \mathbb{R}$).

The *minimal polynomial* of an element $a \in F$ is defined to be the monic annihilating polynomial of a of smallest possible degree.

Prove the following:

(a) The minimal polynomial of an element $a \in F$ is unique whenever it exists. That is, if there is at least one monic annihilating polynomial of a, then only one of these polynomials has smallest possible degree.

(b) The minimal polynomial of an element $a \in F$ is always irreducible if it exists.

(c) If f is the minimal polynomial of an element $a \in F$, then the map

$$S[x]/f \to F,$$
$$\overline{g} \mapsto g[a]$$

is a (well-defined) ring morphism, and is injective.

(d) If f is the minimal polynomial of an element $a \in F$, then the annihilating polynomials of a are precisely the polynomials $g \in S[x]$ that are divisible by f.

3.2 Remark

The minimal polynomial of an $a \in F$ is defined in the exact same way as the minimal polynomial of a square matrix was defined in linear algebra. However, the minimal polynomial of a matrix is not always irreducible, so that part **(b)** of this exercise is specific to fields.

3.3 Solution

...

---

4 Exercise 4

4.1 Problem

Set $S = \mathbb{Q}$ and $F = \mathbb{R}$ in Exercise 3. Let p and q be two positive integers such that none of p, q and pq is a perfect square (i.e., a square in $\mathbb{Z}$). (For example, we can take $p = 5$ and $q = 8$.) Let $a = \sqrt{p} + \sqrt{q} \in F$.

Let f denote the polynomial

$$\left(x^2 - p - q\right)^2 - 4pq = x^4 - 2(p+q)x^2 + (p-q)^2 \in S[x].$$

(a) Show that f is an annihilating polynomial of a (that is, $f[a] = 0$).

(b) Show that f has no rational root.

(c) Show that f is irreducible (in $S[x]$).

(d) Conclude that f is the minimal polynomial of a.

[**Hint:** Part **(c)** is the tricky one. The polynomial f is *even* – meaning that $f[-x] = f$, or, equivalently (since S has characteristic 0) that no odd powers of x appear in f. Use this to argue that if $f = g_1 g_2 \cdots g_k$ is the factorization of f into monic irreducible polynomials, then substituting $-x$ for x into it must yield another factorization $f = f[-x] = g_1[-x]\, g_2[-x] \cdots g_k[-x]$ of f into monic irreducible polynomials (why are they still monic?). Since $S[x]$ is a UFD, the two factorizations must be identical (up to the order of the factors). This narrows down the possibilities for $g_1, g_2, \ldots, g_k$ substantially.]

4.2 Remark

The assumption that none of p, q and pq is a square is not just sufficient, but also necessary for the claim of part **(d)**. For example, if $p = 3$ and $q = 12$ (so that $pq = 36$ is a square), then $\sqrt{p} + \sqrt{q} = \sqrt{3} + \sqrt{12} = 3\sqrt{3}$ has minimal polynomial $x^2 - 27$, and the polynomial f fails to be irreducible.

4.3 Solution

...

---

5 Exercise 5

5.1 Problem

Let p be a prime number. Let F be a finite field of characteristic p. As we know from Lecture 14, this entails that F contains "a copy of $\mathbb{Z}/p$" (that is, a subring isomorphic to $\mathbb{Z}/p$). We identify this copy with $\mathbb{Z}/p$ itself, so that $\mathbb{Z}/p$ is a subring of F. We write S for the field $\mathbb{Z}/p$, and we shall use the terminology from Exercise 3.

Let m be the positive integer satisfying $|F| = p^m$. (We know from Lecture 14 that this m exists.)

Prove the following:

(a) Each $a \in F$ has a minimal polynomial (i.e., there is always at least one monic annihilating polynomial of a).

(b) If the minimal polynomial of an element $a \in F$ has degree k, then $a^{p^k} = a$.

(c) If the minimal polynomial of an element $a \in F$ has degree k, then $k \leq m$.

[**Hint:** Exercise 3 **(c)** can help with parts **(b)** and **(c)** of the present exercise. A size argument might also be useful in **(c)**.]

5.2 Solution

...

---

6 Exercise 6

6.1 Problem

We continue in the setting of Exercise 5. Prove the following:

(a) There exists at least one $a \in F$ such that none of the $m - 1$ powers $a^{p^1}, a^{p^2}, \ldots, a^{p^{m-1}}$ equals a.

(b) There exists at least one monic irreducible polynomial $f \in S[x] = (\mathbb{Z}/p)[x]$ of degree m that satisfies $F \cong S[x]/f$.

(c) Any monic irreducible polynomial $g \in S[x]$ of degree m divides $x^{p^m} - x \in S[x]$.

[**Hint:** For part **(a)**, it helps to notice that $p^m > p^1 + p^2 + \cdots + p^{m-1}$.
For part **(b)**, try to find an element $a \in F$ whose minimal polynomial has degree m.
Part **(c)** is entirely self-contained.]

6.2 Remark

Part **(b)** of this exercise shows that any finite field can be constructed (up to isomorphism) by adjoining a (single) root of an irreducible polynomial to a field of the form $\mathbb{Z}/p$. It also shows that for any prime p and any positive integer m, there exists an irreducible polynomial of degree m over $\mathbb{Z}/p$.

Parts **(b)** and **(c)** can be used in showing that the finite field of a given size is unique up to isomorphism (i.e., any two finite fields of the same size are isomorphic).

6.3 Solution

...

---

7 Exercise 7

7.1 Problem

Let p be a prime number.

(a) Prove that $(1+x)^{ap+c} = (1+x^p)^a (1+x)^c$ in the polynomial ring $(\mathbb{Z}/p)[x]$ for any $a, c \in \mathbb{N}$.

(b) Prove *Lucas's congruence*: Any $a, b \in \mathbb{N}$ and any $c, d \in \{0, 1, \ldots, p-1\}$ satisfy

$$\binom{ap+c}{bp+d} \equiv \binom{a}{b}\binom{c}{d} \mod p.$$

7.2 Solution

...

---

8 Exercise 8

8.1 Problem

Let p be an odd prime. Let ζ be a root of the polynomial $x^4+1 \in (\mathbb{Z}/p)[x]$ in a commutative $\mathbb{Z}/p$-algebra A. Thus, $\zeta^4 = -1$, so that ζ is a unit (with inverse $-\zeta^3$). Let $\tau \in A$ be defined by $\tau = \zeta + \zeta^{-1}$. Prove the following:

(a) We have $\tau^2 = 2$. (Here, 2 stands for $2 \cdot 1_A \in A$.)

(b) We have $\tau^p = \left(\frac{2}{p}\right) \tau$, where $\left(\frac{2}{p}\right)$ means a Legendre symbol.

(c) If $p \equiv \pm 1 \mod 8$ (that is, if p is congruent to 1 or to -1 modulo 8), then $\tau^p = \tau$.

(d) If $p \equiv \pm 3 \mod 8$ (that is, if p is congruent to 3 or to -3 modulo 8), then $\tau^p = -\tau$.

(e) Conclude the *Second Supplementary Law to Quadratic Reciprocity*, which says that

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \mod 8; \\ -1, & \text{if } p \equiv \pm 3 \mod 8. \end{cases} \tag{1}$$

[**Hint:** For part **(b)**, start out by writing $\tau^p = \left(\tau^2\right)^{(p-1)/2} \tau$.]

8.2 Remark

The right hand side of (1) is also commonly written as $(-1)^{\left(p^2-1\right)/8}$.

8.3 Solution

...

---

9 Exercise 9

9.1 Problem

Let R be a commutative ring. Let P be the polynomial ring $R[x, y]$.

Fix $N \in \mathbb{N}$. Let P_N be the R-submodule

$$\{f \in P \mid f = 0 \text{ or } \deg f < N\}$$

of P. (This is an R-submodule, since it is the span of the family $\left(x^i y^j\right)_{(i,j) \in \mathbb{N}^2;\ i+j<N}$.)

(a) Consider the R-algebra morphism

$$S : P \to R[x], \qquad f \mapsto f\left(x, x^N\right).$$

(This is the map that substitutes x^N for y in any polynomial $f \in P$. It is an R-algebra morphism, as we know from Lecture 11.)

Prove that the restriction of S to P_N is injective.

From now on, assume that R is a field.

(b) Let $f \in P_N$ be such that the polynomial $S(f) \in R[x]$ is irreducible. Show that $f \in P = R[x, y]$ is irreducible.

9.2 Remark

The converse of part **(b)** does not hold. For example, if $R = \mathbb{Q}$ and $N = 2$, then the polynomial $f := 1 + 2x + y \in P$ is irreducible, but the polynomial $S(f) = 1 + 2x + x^2 = (1+x)^2 \in R[x]$ is not.

9.3 Solution

...

---

10 Exercise 10

10.1 Problem

Let R be a commutative ring. Let $f \in R[x]$ be a polynomial. Prove that f is a unit of the ring $R[x]$ if and only if[1]

- the coefficient $[x^0] f$ is a unit of R, and
- all the remaining coefficients $[x^1] f, [x^2] f, [x^3] f, \ldots$ of f are nilpotent.

[**Hint:** Recall the result (from Exercise 7 **(c)** on homework set #1) that the nilpotent elements of a commutative ring form an ideal, as well as the result (from Exercise 1 on homework set #2) that the difference of a unit and a nilpotent element is always a unit (in a commutative ring). This should help with the "if" direction. For the "only if" direction, let $f = f_0 x^0 + f_1 x^1 + \cdots + f_n x^n \in R[x]$ be a unit and $g = g_0 x^0 + g_1 x^1 + \cdots + g_m x^m \in R[x]$ be its inverse. Use induction on r to show that $f_n^{r+1} g_{m-r} = 0$ for each $r \in \{0, 1, \ldots, m\}$. Use this to conclude that f_n is nilpotent.]

10.2 Remark

This exercise precisely delineates the phenomenon of nonconstant polynomials that have inverses (such as the polynomial $\overline{1} + \overline{2}x \in (\mathbb{Z}/4)[x]$). In particular, it shows that this requires R not only to have zero-divisors (i.e., not be an integral domain), but also to have nonzero nilpotent elements (so, e.g., it cannot happen for $R = \mathbb{Z}/6$).

10.3 Solution

...

References

[1]Recall that $[x^i] f$ denotes the coefficient of the monomial x^i in f.