

## 2021 Fall Honors Algebra Exercise 4 (due on November 9)

For submission of homework, please finish the 20 True/False problems, and choose 10 problems from the standard ones and 5 problems from the more difficult ones. Mark the question numbers clearly.

[A] = Artin, [DF] = Dummit and Foote, [DN] = Ding and Nie (Chinese), [H] = Hungerford.

All rings contain 1 and  $1 \neq 0$  in these rings. Moreover, homomorphisms always take 1 to 1.

4.1. **True/False questions.** (Only write T or F when submitting the solutions.)

- (1) In a ring  $R$ , if  $I_1 \subseteq I_2 \subseteq \dots$  be an increasing sequence of proper ideals (meaning  $I_i \neq R$  for each  $i$ ), then  $\cup_{i=1}^{\infty} I_i$  is a proper ideal of  $R$ .
- (2) In a commutative ring  $R$ , the intersection of two ideals  $I$  and  $J$  always contains  $IJ$ .  
For (3)–(7) below, let  $\varphi : R \rightarrow R'$  be a surjective homomorphism of commutative rings.
  - (3) if  $a \in R$  is a zero-divisor, then  $\varphi(a) \in R'$  is a zero-divisor;
  - (4) if  $R$  is an integral domain, then  $\varphi(R) = R'$  is an integral domain;
  - (5) if  $R'$  is an integral domain, then  $R$  is an integral domain;
  - (6) if  $u \in R$  is a unit, then  $\varphi(u)$  is a unit in  $R'$ ;
  - (7) if  $\varphi(u) \in R'$  is a unit, then  $u$  is a unit in  $R$ .
- (8) In a commutative ring  $R$ ,  $x^2 - 1$  has exactly two zeros:  $x = \pm 1$ .
- (9) If  $R$  is a UFD, then every element  $p(x) \in R[x]$  that is irreducible in  $\text{Frac}(R)[x]$  is irreducible in  $R[x]$ .
- (10) If  $R$  is a PID, then  $R[x]$  is a PID.
- (11) If  $R$  is a PID, then for any ideal  $I$  of  $R$ ,  $R/I$  is a PID.
- (12) Since  $5 = (1+2i)(1-2i) = (2-i)(2+i)$  are different factorizations of 5 in  $\mathbb{Z}[i]$ ,  $\mathbb{Z}[i]$  is not a UFD.
- (13) If  $P_1$  and  $P_2$  are prime ideals in a commutative ring  $R$ , then  $P_1 + P_2$  is a prime ideal.
- (14) If  $p$  is a prime element in an integral domain  $D$ , then  $p$  is an irreducible element.
- (15)  $\mathbb{Z}[\sqrt{-5}]$  is an integral domain but not a PID.

4.2. **Warm-up questions.** (Do not submit solutions for the following questions)

**Problem 4.2.1.** [DF, page 278, problem 7]

Find a generator for the ideal  $(85, 1 + 13i)$  in  $\mathbb{Z}[i]$ , i.e. a greatest common divisor for 85 and  $1 + 13i$ , by Euclidean Algorithm.

**Problem 4.2.2.** (Math behind Public Key Code: easy version)

[DF, page 279, problem 12]

Let  $N$  be a positive integer. Let  $M$  be an integer relatively prime to  $N$  and let  $d$  be an integer relatively prime to  $\varphi(N)$ , where  $\varphi$  denotes Euler's  $\varphi$ -function. Prove that if  $M_1 = M^d \pmod{N}$  then  $M = M^{d'} \pmod{N}$  where  $d'$  is the inverse of  $d \pmod{\varphi(N)}$ :  $dd' = 1 \pmod{\varphi(N)}$ .

Remark: This result is the basis for a standard Public Key Code. Suppose  $N = pq$  is the product of two distinct large primes (each on the order of 100 digits, for example). If  $M$  is a message, then  $M_1 = M^d \pmod{N}$  is a scrambled (encoded) version of  $M$ , which can be unscrambled (decoded) by computing  $M_1^{d'} \pmod{N}$  (these powers can be computed quite easily even for large values of  $M$  and  $N$  by successive squarings; not by directly checking one-by-one!). The values of  $N$  and  $d$  (but not  $p$  and  $q$ ) are made publicly known (hence the name) and then anyone with a message  $M$  can send their encoded message  $M^d \pmod{N}$ . To decode the message it seems necessary to determine  $d'$ , which requires the determination of the value  $\varphi(N) = \varphi(pq) = (p-1)(q-1)$  (no one has as yet proved that there is no other decoding scheme, however). The success of this method as a code rests on the necessity of determining the factorization of  $N$  into primes, for which no sufficiently efficient algorithm exists (for example, the most naive method of checking all factors up to  $\sqrt{N}$  would here require on the order of  $10^{100}$  computations, or approximately 300 years even at 10 billion computations per second, and of course one can always increase the size of  $p$  and  $q$ ).

So one may view this as an application of the multiplication group  $(\mathbb{Z}/p\mathbb{Z})^\times$ . As modern mathematics progresses, there are analogous public key code schemes available. One typical way is to use so called "elliptic curves", solutions to equations like  $y^2 = x^3 + ax + b$  modulo a large prime  $p$ , where  $a, b \in \mathbb{Z}/p\mathbb{Z}$ . Among many other benefits of this new type of coding system is that: people who want to decode it need to study much more beyond abstract algebra, :). Indeed, who understands higher mathematics may tend to have less motivation to do harmful things.

**Problem 4.2.3.** [DF, page 282, problem 3]

Prove that a quotient of a P.I.D. by a prime ideal is again a P.I.D.

**Problem 4.2.4.** [DF, page 256, problem 6]

Prove that  $R$  is a division ring if and only if its only left ideals are  $(0)$  and  $R$ . (The analogous result holds when "left" is replaced by "right.")

**Problem 4.2.5** (DF, page 257, problem 11). Assume  $R$  is commutative. Let  $I$  and  $J$  be ideals of  $R$  and assume  $P$  is a prime ideal of  $R$  that contains  $IJ$  (for example, if  $P$  contains  $I \cap J$ ). Prove either  $I$  or  $J$  is contained in  $P$ .

**Problem 4.2.6.** [DF, page 293, problem 3]

Determine all representations of the integer  $2130797 = 17^2 \cdot 73 \cdot 101$  as a sum of two squares.

**Problem 4.2.7.** [DF, page 298, problem 5]

Prove that  $(x, y)$  and  $(2, x, y)$  are prime ideals in  $\mathbb{Z}[x, y]$  but only the latter ideal is a maximal ideal.

**Problem 4.2.8.** [DF, page 301, problem 5]

Exhibit all the ideals in the ring  $F[x]/(p(x))$ , where  $F$  is a field and  $p(x)$  is a polynomial in  $F[x]$  (describe them in terms of the factorization of  $p(x)$ ).

**Problem 4.2.9.** [DF, page 311, problem 1]

Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation  $\mathbb{F}_p$  denotes the finite field  $\mathbb{Z}/p\mathbb{Z}$  for  $p$  a prime.

- (1)  $x^2 + x + 1$  in  $\mathbb{F}_p[x]$ .
- (2)  $x^3 + x + 1$  in  $\mathbb{F}_3[x]$ .
- (3)  $x^4 + 1$  in  $\mathbb{F}_5[x]$ .
- (4)  $x^4 + 10x^2 + 1$  in  $\mathbb{Z}[x]$ .

**Problem 4.2.10.** [DF, page 312, problem 13]

Prove that  $x^3 + nx + 2$  is irreducible over  $\mathbb{Z}$  for all integers  $n \neq 1, -3, -5$ .

**Problem 4.2.11.** Consider  $\mathbb{Z}[x]$ .

- (1) Is  $\mathbb{Z}[x]$  a UFD? Why?
- (2) Show that  $\{a + xf(x) | a \in 2\mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$  is an ideal in  $\mathbb{Z}[x]$ .
- (3) Is  $\mathbb{Z}[x]$  a PID?
- (4) Is  $\mathbb{Z}[x]$  a Euclidean domain? Why?

4.3. Standard questions. (Please choose 10 problems from the following questions)

**Problem 4.3.1.** [DF, page 267, problem 1]

Let  $R$  be a ring with identity  $1 \neq 0$ . An element  $e \in R$  is called an idempotent if  $e^2 = e$ . Assume  $e$  is an idempotent in  $R$  and  $er = re$  for all  $r \in R$ . Prove that  $Re$  and  $R(1 - e)$  are two-sided ideals of  $R$  and that  $R \cong Re \times R(l - e)$ . Show that  $e$  and  $1 - e$  are identities for the subrings  $Re$  and  $R(l - e)$  respectively.

**Problem 4.3.2.** (1) Show that the units in the product of commutative rings is the product of sets of units, i.e. for two commutative unital rings  $R_1$  and  $R_2$ , we have  $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$ .

(2) From this deduce that, if  $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  is the prime factorization of a positive integer, we have

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times.$$

(3) Show that each  $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$  is a cyclic group of order  $p_i^{\alpha_i-1}(p_i - 1)$ .

**Problem 4.3.3.** [DF, page 283, problem 6]

Let  $R$  be an integral domain and suppose that every prime ideal in  $R$  is principal. This exercise proves that every ideal of  $R$  is principal. i.e.,  $R$  is a P.I.D.

- (1) Assume that the set of ideals of  $R$  that are not principal is nonempty and prove that this set has a maximal element under inclusion (which, by hypothesis, is not prime). [Use Zorn's Lemma.]
- (2) Let  $I$  be an ideal which is maximal with respect to being nonprincipal, and let  $a, b \in R$  with  $ab \in I$  but  $a \notin I$  and  $b \notin I$ . Let  $I_a = (I, a)$  be the ideal generated by  $I$  and  $a$ , let  $I_b = (I, b)$  be the ideal generated by  $I$  and  $b$ , and define  $J = \{r \in R \mid rI_a \subseteq I\}$ . Prove that  $I_a = (\alpha)$  and  $J = (\beta)$  are principal ideals in  $R$  with  $I \subsetneq I_b \subseteq J$  and  $I_aJ = (\alpha\beta) \subseteq I$ .
- (3) If  $x \in I$  show that  $x = s\alpha$  for some  $s \in J$ . Deduce that  $I = I_aJ$  is principal, a contradiction, and conclude that  $R$  is a P.I.D.

**Problem 4.3.4.** [DF, page 258, problems 30 and 31]

- (1) Let  $I$  be an ideal of the commutative ring  $R$  and define

$$\text{rad}(I) = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\}$$

called the *radical of  $I$* . (In many other references, we write  $\sqrt{I}$  instead.) Prove that  $\text{rad}(I)$  is an ideal containing  $I$  and that  $\text{rad}(I)/I$  is the nilradical of the quotient ring  $R/I$ , i.e.,  $(\text{rad}(I))/I = \mathfrak{N}(R/I)$  (see Problem 3.3.16).

- (2) An ideal  $I$  of  $R$  is called a *radical ideal* if  $\text{rad}(I) = I$ . Prove that every prime ideal of  $R$  is a radical ideal.

**Problem 4.3.5.** [DF, page 259, problem 37]

A commutative ring  $R$  is called a local ring if it has a unique maximal ideal. Prove that if  $R$  is a local ring with maximal ideal  $M$  then every element of  $R - M$  is a unit. Prove conversely that if  $R$  is a commutative ring with 1 in which the set of nonunits forms an ideal  $M$ , then  $R$  is a local ring with unique maximal ideal  $M$ .

(Local rings are important concepts in commutative algebra. Without getting into much detail, the idea is that, like we study one-prime-by-another when solving integer coefficient polynomial equations, we may study elements or properties of a ring by working with each prime ideal. There is a localization process that “zoom-in” the study at one prime and

produce a local ring as above. The local ring, in some ways, is a best approximation of fields that is still a just a ring.)

**Problem 4.3.6.** [DF, page 283, problem 7] and [DF, page 294, problem 11]

An integral domain  $R$  in which every ideal generated by two elements is principal (i.e., for every  $a, b \in R$ ,  $(a, b) = (d)$  for some  $d \in R$ ) is called a *Bezout Domain*.

- (1) Prove that the integral domain  $R$  is a Bezout Domain if and only if every pair of elements  $a, b$  of  $R$  has a g.c.d.  $d \in R$  that can be written as an  $R$ -linear combination of  $a$  and  $b$ , i.e.,  $d = ax + by$  for some  $x, y \in R$ .
- (2) Prove that every finitely generated ideal of a Bezout Domain is principal. (In particular, a Bezout Domain is a non-noetherian version of P.I.D.)
- (3) Let  $F$  be the fraction field of the Bezout Domain  $R$ . Prove that every element of  $F$  can be written in the form  $a/b$  with  $a, b \in R$  and  $a$  and  $b$  relatively prime.
- (4) Prove that  $R$  is a P.I.D. if and only if  $R$  is a U.F.D. that is also a Bezout Domain.

**Problem 4.3.7.** (continued with the previous problem)

Let  $F[x, y_1, y_2, \dots]$  be the polynomial ring in the infinite set of variables  $x, y_1, y_2, \dots$  over the field  $F$ , and let  $I$  be the ideal  $(x - y_1^2, y_1 - y_2^2, \dots, y_i - y_{i+1}^2, \dots)$  in this ring. Define  $R$  to be the ring  $F[x, y_1, y_2, \dots]/I$ , so that in  $R$  the square of each  $y_{i+1}$  is  $y_i$  and  $y_1^2 = x$  modulo  $I$ , i.e.,  $x$  has a  $2^i$ th root, for every  $i$ . Denote the image of  $y_i$  in  $R$  as  $x^{1/2^i}$ . Let  $R_n$  be the subring of  $R$  generated by  $F$  and  $x^{1/2^n}$ .

- (1) Prove that  $R_1 \subseteq R_2 \subseteq \dots$  and that  $R$  is the union of all  $R_n$ , i.e.,  $R = \bigcup_{n=1}^{\infty} R_n$ .
- (2) Prove that  $R_n$  is isomorphic to a polynomial ring in one variable over  $F$ , so that  $R_n$  is a P.I.D. Deduce that  $R$  is a Bézout Domain. (There are hints on the book which I omitted here.)
- (3) Prove that the ideal generated by  $x, x^{1/2}, x^{1/4}, \dots$  in  $R$  is not finitely generated (so  $R$  is not a P.I.D.).

**Problem 4.3.8.** (from a discussion with Junyi Xie)

Let  $p$  be a prime number. Consider the following subset of polynomials

$$S = \left\{ \sum_{n \geq 0} a_n x^{p^n} \mid a_n \in \mathbb{F}_p \right\}.$$

Show that  $S$  is closed under composition  $f \circ g(x)$ .

Prove that  $S$  together with the natural addition and composition (not the multiplication) is a ring, and isomorphic to the polynomial ring  $\mathbb{F}_p[x]$ .

(Can you construct a natural map from  $\mathbb{F}_p[x] \rightarrow S$  that is easy to describe and contains the Frobenius map?)

**Problem 4.3.9.** [DF, page 257, problem 13]

Let  $\varphi : R \rightarrow S$  be a homomorphism of commutative rings with 1 (and  $\varphi(1_R) = 1_S$ ).

- (1) Prove that if  $P$  is a prime ideal of  $S$  then  $\varphi^{-1}(P)$  is a prime ideal of  $R$ . In particular, if  $R$  is a subring of  $S$ , then intersection of a prime ideal of  $S$  with  $R$  is a prime ideal of  $R$ .
- (2) Prove that if  $M$  is a maximal ideal of  $S$  and  $\varphi$  is surjective then  $\varphi^{-1}(M)$  is a maximal ideal of  $R$ . Give an example to show that this need not be the case if  $\varphi$  is not surjective.

(Remark: this is a very important exercise, I highly recommend you work out this problem.)

**Problem 4.3.10.** [DF, page 283, problem 5]

Let  $R$  be the quadratic integer ring  $\mathbb{Z}[\sqrt{-5}]$ . Define the ideals  $I_2 = (2, 1 + \sqrt{-5})$ ,  $I_3 = (3, 1 + \sqrt{-5})$ , and  $I'_3 = (3, 1 - \sqrt{-5})$ .

- (1) Prove that  $I_2$ ,  $I_3$ , and  $I'_3$  are non-principal ideals in  $R$ .
- (2) Prove that the product of two non-principal ideals can be principal by showing that if it is the principal ideal generated by 2, i.e.,  $I_2^2 = (2)$ .
- (3) Prove similarly that  $I_2 I_3 = (1 + \sqrt{-5})$  and  $I_2 I'_3 = (1 - \sqrt{-5})$  are principal. Conclude that the principal ideal (6) is the product of 4 ideals:  $(6) = I_2^2 I_3 I'_3$ .

Remark: In fact, one can show that nonzero ideals in  $R$  has two kinds: principal ones and non-principal ones, and the product of any two non-principal ideals is a principal ideal. This is a particular case that the “ideal class group of  $R$  is  $\mathbb{Z}/2\mathbb{Z}$ ”.

**Problem 4.3.11.** [DF, page 293, problem 6]

(1) Let  $q \in \mathbb{Z}$  be a prime with  $q \equiv 3 \pmod{4}$ . Prove that the quotient ring  $\mathbb{Z}[i]/(q)$  is a field with  $q^2$  elements.

(2) Let  $p \in \mathbb{Z}$  be a prime with  $p \equiv 1 \pmod{4}$  and write  $p = \pi\bar{\pi}$  as its factorization into irreducible elements. Show that the hypotheses for the Chinese Remainder Theorem are satisfied and that  $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi})$  as rings. Show that the quotient ring  $\mathbb{Z}[i]/(p)$  has order  $p^2$  and conclude that  $\mathbb{Z}[i]/(\pi)$  and  $\mathbb{Z}[i]/(\bar{\pi})$  are both fields of order  $p$ .

**Problem 4.3.12.** [DF, page 298, problem 8]

Let  $F$  be a field and let  $R = F[x, x^2y, x^3y^2, \dots, x^n y^{n-1}, \dots]$  be a subring of the polynomial ring  $F[x, y]$ .

- (1) Prove that the fields of fractions of  $R$  and  $F[x, y]$  are the same.
- (2) Prove that  $R$  contains an ideal that is not finitely generated.

**Problem 4.3.13.** [DN, page 156, problem 22]

In the Gaussian integer ring  $\mathbb{Z}[i]$ , determine whether

$$f(x) = x^4 + (8+i)x^3 + (3-4i)x + 5$$

is irreducible or not.

**Problem 4.3.14.** [DF, page 299, problem 17]

Let  $R$  be a commutative ring. An ideal  $I$  in  $R[x_1, \dots, x_n]$  is called a *homogeneous ideal* if whenever  $p \in I$  then each homogeneous component of  $p$  is also in  $I$ . Prove that an ideal is a homogeneous ideal if and only if it may be generated by homogeneous polynomials.

**Problem 4.3.15.** [DF, page 206, problem 4]

Let  $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$  be the set of polynomials in  $x$  with rational coefficients whose constant term is an integer.

- (1) Prove that  $R$  is an integral domain and its units are  $\pm 1$ .
- (2) Show that the irreducibles in  $R$  are  $\pm p$  where  $p$  is a prime in  $\mathbb{Z}$  and the polynomials  $f(x)$  that are irreducible in  $\mathbb{Q}[x]$  and have constant term  $\pm 1$ . Prove that these irreducibles are prime in  $R$ .
- (3) Show that  $x$  cannot be written as the product of irreducibles in  $R$  (in particular,  $x$  is not irreducible) and conclude that  $R$  is not a U.F.D.
- (4) Show that  $x$  is not a prime in  $R$  and describe the quotient ring  $R/(x)$ .

**Problem 4.3.16.** [DF, page 311, problem 8]

Prove that  $K_1 = \mathbb{F}_{11}[x]/(x^2 + 1)$  and  $K_2 = \mathbb{F}_{11}[y]/(y^2 + 2y + 2)$  are both fields with 121 elements. Prove that the map which sends the element  $p(\bar{x})$  of  $K_1$  to the element  $p(\bar{y} + 1)$  of  $K_2$  (where  $p$  is any polynomial with coefficients in  $\mathbb{F}_{11}$ ) is well defined and gives a ring (hence field) isomorphism from  $K_1$  to  $K_2$ .

**Problem 4.3.17.** [DF, page 312, problem 11]

Prove that  $x^2 + y^2 - 1$  is irreducible in  $\mathbb{Q}[x, y]$ .

**Problem 4.3.18.** [DF, page 312, problem 16]

Let  $F$  be a field and let  $f(x)$  be a polynomial of degree  $n$  in  $F[x]$ . The polynomial  $g(x) = x^n f(1/x)$  is called the reverse of  $f(x)$ .

- (1) Describe the coefficients of  $g$  in terms of the coefficients of  $f$ .
- (2) Prove that  $f$  is irreducible if and only if  $g$  is irreducible.

Remark: If  $A$  is an  $n \times n$ -matrix, how do you relate the characteristic polynomial  $\det(xI_n - A)$  and the so-called characteristic power series  $\det(I_n - xA)$ ?

**Problem 4.3.19.** [H, page 157, problem 8]

- (1) The polynomial  $x + 1$  is a unit in the power series ring  $\mathbb{Z}[[x]]$ , but is not a unit in  $\mathbb{Z}[x]$ .
- (2)  $x^2 + 3x + 2$  is irreducible in  $\mathbb{Z}[[x]]$  but not in  $\mathbb{Z}[x]$ .

**Problem 4.3.20.** [DF, page 315, problem 3]

Let  $p$  be an odd prime in  $\mathbb{Z}$  and let  $n$  be a positive integer. Prove that  $x^n - p$  is irreducible over  $\mathbb{Z}[i]$ .

**Problem 4.3.21** (Classical results). Let  $R$  be a commutative ring.

- (1) Recall that the *nil-radical*  $\mathfrak{N}$  is the ideal of  $R$  consisting of elements  $x$  in  $R$  such that  $x^N = 0$  for some  $N \in \mathbb{N}$ . Show that  $\mathfrak{N}$  is the intersection of all prime ideals of  $R$  is contained in  $\mathfrak{N}$ . (Remark: it can be shown that the intersection of all prime ideals is precisely  $\mathfrak{N}$ .)
- (2) The *Jacobson radical*  $J$  of  $R$  is the intersection of all maximal ideals of  $R$ . Show that if  $a \in J$  then  $1 + a$  is a unit in  $R$ .

**4.4. More difficult questions.** (Please choose 5 problems from the following questions)

**Problem 4.4.1.** [DN, page 129, problem 1]

Let  $R$  be a ring with  $1 \neq 0$ . For two elements  $a, b \in R$ , if  $1 - ab$  is a unit, then  $1 - ba$  is a unit.

(I have a nice explanation of the proof, but I don't want to ruin it; so I leave the hint to the end of the file. It's up to you whether to use it.)

**Problem 4.4.2.** [DF, page 306, problem 5]

Keep the notation as in Problem 4.3.15. Let  $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ .

- (1) Suppose that  $f(x), g(x) \in \mathbb{Q}[x]$  are two nonzero polynomials with rational coefficients and that  $x^r$  is the largest power of  $x$  dividing both  $f(x)$  and  $g(x)$  in  $\mathbb{Q}[x]$ , (i.e.,  $r$  is the degree of the lowest order term appearing in either  $f(x)$  or  $g(x)$ ). Let  $f_r$  and  $g_r$  be the coefficients of  $x^r$  in  $f(x)$  and  $g(x)$ , respectively (one of which is nonzero by definition of  $r$ ). Then  $\mathbb{Z}f_r + \mathbb{Z}g_r = \mathbb{Z}d_r$  for some nonzero  $d_r \in \mathbb{Q}$ . Prove that there is a polynomial  $d(x) \in \mathbb{Q}[x]$  that is a g.c.d. of  $f(x)$  and  $g(x)$  in  $\mathbb{Q}[x]$  and whose term of minimal degree is  $d_r x^r$ .
- (2) Prove that  $f(x) = d(x)q_1(x)$  and  $g(x) = d(x)q_2(x)$  where  $q_1(x)$  and  $q_2(x)$  are elements of the subring  $R$  of  $\mathbb{Q}[x]$ .
- (3) Prove that  $d(x) = a(x)f(x) + b(x)g(x)$  for polynomials  $a(x), b(x)$  in  $R$ .
- (4) Conclude from (a) and (b) that  $Rf(x) + Rg(x) = Rd(x)$  in  $\mathbb{Q}[x]$  and use this to prove that  $R$  is a Bezout Domain.
- (5) Show that (d), the results of the previous exercise imply that  $R$  must contain ideals that are not principal (hence not finitely generated). Prove that in fact  $I = x\mathbb{Q}[x]$  is an ideal of  $R$  that is not finitely generated.

**Problem 4.4.3.** [DF, page 311, problem 3]

Show that the polynomial  $(x-1)(x-2)\cdots(x-n)-1$  is irreducible over  $\mathbb{Z}$  for all  $n \geq 1$ .

(There is a hint in the book; I leave it to you to decide whether to look at it. This is a little tricky.)

**Problem 4.4.4.** [DF, page 311, problem 10]

Prove that  $p(x) = x^4 - 4x^2 + 8x + 2$  is irreducible over the quadratic field  $F = \mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} | a, b \in \mathbb{Q}\}$ .

**Problem 4.4.5.** Let  $A, B \in \mathbb{Q}^\times$  be rational numbers. Consider the quaternion ring

$$D_{A,B,\mathbb{R}} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

in which the multiplication satisfies relations:  $i^2 = A$ ,  $j^2 = B$ , and  $ij = -ji = k$ .

- (1) Represent  $jk$ ,  $ik$ ,  $k^2$  in terms of elements in  $D_{A,B,\mathbb{R}}$ .
- (2) When  $A, B > 0$ , show that  $D_{A,B,\mathbb{R}}$  is isomorphic to  $\text{Mat}_{2 \times 2}(\mathbb{R})$ , given by

$$i \leftrightarrow \begin{pmatrix} \sqrt{A} & 0 \\ 0 & -\sqrt{A} \end{pmatrix}, \quad j \leftrightarrow \begin{pmatrix} 0 & B \\ 1 & 0 \end{pmatrix}.$$

- (3) Show that  $D_{A,B,\mathbb{R}}$  is isomorphic to  $\mathbb{H}$  if and only if  $A, B < 0$ , and is isomorphic to  $\text{Mat}_{2 \times 2}(\mathbb{R})$  if at least one of  $A$  and  $B$  is positive.
- (4) Why is  $\text{Mat}_{2 \times 2}(\mathbb{R})$  not isomorphic to  $\mathbb{H}$ ?

**Problem 4.4.6.** Let  $A, B \in \mathbb{Q}^\times$  be rational numbers. Consider the quaternion ring

$$D_{A,B,\mathbb{Q}} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Q}\}$$

in which the multiplication satisfies relations:  $i^2 = A$ ,  $j^2 = B$ , and  $ij = -ji = k$ .

- (1) Show that if either  $A$  or  $B$  is a square in  $\mathbb{Q}$ , then  $D_{A,B,\mathbb{Q}}$  is isomorphic to  $\text{Mat}_{2 \times 2}(\mathbb{Q})$ .
- (2) Prove that  $D_{A,B,\mathbb{Q}}$  is isomorphic to  $\text{Mat}_{2 \times 2}(\mathbb{Q})$  if and only if  $x^2 = Ay^2 + Bz^2$  has a nonzero (meaning not all zero) solution in  $\mathbb{Q}$ .

**Problem 4.4.7.** [Alibaba 2021]

Let  $p$  be a prime number and let  $\mathbb{F}_p$  be the finite field with  $p$  elements. Consider an automorphism  $\tau$  of the polynomial ring  $\mathbb{F}_p[x]$  given by

$$\tau(f)(x) = f(x+1).$$

Let  $R$  denote the subring of  $\mathbb{F}_p[x]$  consisting of those polynomials  $f$  with  $\tau(f) = f$ . Find a polynomial  $g \in \mathbb{F}_p[x]$  such that  $\mathbb{F}_p[x]$  is a free module over  $R$  with basis  $g, \tau(g), \dots, \tau^{p-1}(g)$  (in other words, every element of  $\mathbb{F}_p[x]$  can be uniquely written as a “linear combination”

$$a_0g + a_1\tau(g) + \dots + a_{p-1}\tau^{p-1}(g)$$

with  $a_0, \dots, a_{p-1} \in R$ .

**Problem 4.4.8.** Let  $S_3$  be the symmetric group on 3 letters and let  $R$  be the group ring  $R = \mathbb{Z}[S_3]$ .

- (1) Write down a nonzero element in  $R$  which is a zero-divisor.
- (2) Write down an element in the center of  $R$  which is not in  $\mathbb{Z}$ .

**Problem 4.4.9.** [DN, page 134, problem 67]

Let  $G$  be an abelian group and  $\eta, \xi$  be endomorphisms of  $G$  (namely homomorphisms from  $G$  to itself). Define the product and sum of  $\eta$  and  $\xi$  to be

$$\eta \cdot \xi(a) = \eta(\xi(a)), \quad (\eta + \xi)(a) = \eta(a) + \xi(a)$$

for  $a \in G$ . Verify that  $\eta + \xi$  is a homomorphism from  $G$  to itself. This two operations on the set of all endomorphisms of  $G$ :  $\text{End}(G)$  defines a structure of rings, called the *endomorphism ring*.

Determine the endomorphism ring of the following:

- (1)  $(\mathbb{Z}, +)$
- (2)  $Z_n$
- (3)  $(Z_p)^n = Z_p \times \dots \times Z_p$  (where  $p$  is a prime).

**Problem 4.4.10.** Imitate the discussion of Gaussian integers for  $R = \mathbb{Z}[\zeta_3]$  with  $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ .

- (1) Show that a prime  $p$  can be written as  $p = a^2 + ab + b^2$  with  $a, b \in \mathbb{Z}$  if and only if  $p \equiv 3$  or  $p \equiv 1 \pmod{3}$ .
- (2) Classify irreducible elements in  $R = \mathbb{Z}[\zeta_3]$ .

Hint for Problem 4.4.1: Consider a Taylor expansion  $(1 - ab)^{-1} = 1 + ab + abab + \dots$  and relate this to  $(1 - ba)^{-1}$ . Then, you just have to make sense of what you have computed.