Math 611 Homework 4

Paul Hacking

November 4, 2019

Reading: Dummit and Foote, Sections 6.3, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6.

Justify your answers carefully (complete proofs are expected). All rings are assumed commutative with 1 unless explicitly stated otherwise.

(1) Let $R = (\mathbb{Z}/2\mathbb{Z})[x]/(x^2+x+1)$.

(a) Writing $\alpha = x+(x^2+x+1)$ for the image of x in R, list the elements of R and write out the addition and multiplication tables for R.

(b) Show that the abelian group $(R,+)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and $(R \setminus \{0\}, \cdot)$ is an abelian group isomorphic to $\mathbb{Z}/3\mathbb{Z}$. In particular deduce that R is a field of order 4.

(2) Let R be a ring.

(a) Show that there is a unique homomorphism $\varphi\colon \mathbb{Z} \to R$ and describe it explicitly.

(b) Let $\ker(\phi) = (n)$, some $n \in \mathbb{Z}_{\geq 0}$. The integer n is called the *characteristic* of R. Show that if R is an integral domain then either $n = 0$ or n is a prime.

(3) Identify the quotient ring as explicitly as possible.

(a) $\mathbb{Z}[x]/(x-7)$.

(b) $\mathbb{R}[x]/(x^2+9)$.

(c) $\mathbb{Q}[x]/(x^2+5x-14)$.

(d) $\mathbb{Z}[i]/(3+4i)$.

(e) $\mathbb{Z}[x]/(6, 2x-1)$.

(f) $\mathbb{Z}[x]/(2x^2 - 4, 4x + 5)$.

(g) $\mathbb{Z}[x]/(x^2 - 3, 2x - 4)$.

(h) $\mathbb{Z}[x]/(x^2 + 3, 5)$.

(4) Identify the kernel and the image of each of the following homomorphisms explicitly.

(a) $\varphi\colon \mathbb{C}[x, y] \to \mathbb{C}[t]$, $\varphi(f(x, y)) = f(t^2, t^3)$.

(b) $\psi\colon \mathbb{C}[x, y] \to \mathbb{C}[t]$, $\psi(f(x, y)) = f(t^2 - 1, t(t^2 - 1))$.

(5) Show that a principal ideal in $\mathbb{Z}[x]$ is not maximal.

(6) Determine the automorphism group of the ring $\mathbb{Z}[x]$.

(7) Let R and S be rings. Prove that the ideals of the direct product $R \times S$ are the subsets of the form $I \times J$ where I is an ideal of R and J is an ideal of S.

(8) Let R be a finite ring. Show that if R is an integral domain then R is a field.

(9) Classify rings of order 15.

(10) Let R be a ring of characteristic p, a prime (see Q2 above for the definition of the characteristic of a ring).

(a) Show that the map

$$F\colon R \to R, \quad a \mapsto a^p$$

is a ring homomorphism, called the *Frobenius homomorphism*.

(b) Describe F explicitly in the case $R = (\mathbb{Z}/p\mathbb{Z})[x]$, the ring of polynomials in the variable x with coefficients in $\mathbb{Z}/p\mathbb{Z}$.

(11) An element a of a ring R is called *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$.

(a) Show that if a is nilpotent then $1 + a$ is a unit.

(b) Show that the set N of all nilpotent elements is an ideal of R (called the *nilradical*).

(c) Show that R/N does not contain any nonzero nilpotent elements.

(12) Let F be a field. Show that there is a minimal subfield F_0 of F, called the *prime subfield*, which is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

(13) We say a ring R is a *local ring* if there is a unique maximal ideal $M \subset R$.

(a) Let $n \in \mathbb{N}$, $n > 1$. Show that $\mathbb{Z}/n\mathbb{Z}$ is a local ring if and only if n is a power of a prime.

(b) Suppose R is a local ring with maximal ideal M. Show that the set $R^\times$ of units of R is the complement $R \setminus M$ of the maximal ideal M.

(c) Conversely, suppose R is a ring and $I \subsetneq R$ is a proper ideal such that every element of the complement $R \setminus I$ is a unit. Show that R is a local ring with maximal ideal I.

(14) The *formal power series ring* $\mathbb{C}[[x]]$ has elements

$$f = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x + \cdots$$

where $a_i \in \mathbb{C}$ for each i. (The adjective *formal* indicates that we do not require that the series converges for any nonzero value of x in $\mathbb{C}$. That is, using the terminology of complex analysis, the radius of convergence may be equal to zero.) Addition and multiplication of formal power series are defined in the obvious way, e.g,

$$\left(\sum a_i x^i\right) \cdot \left(\sum b_i x^i\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \cdots.$$

(Notice that the coefficients of the product are finite sums, so the product is well-defined.)

(a) Show that $\mathbb{C}[[x]]$ is a local ring with maximal ideal $M = (x)$.

(b) What are the ideals of $\mathbb{C}[[x]]$?

(c) Show that the fraction field of $\mathbb{C}[[x]]$ can be identified with the ring $\mathbb{C}((x))$ of *formal Laurent series*: formal expressions

$$f = \sum_{i=n}^{\infty} a_i x^i$$

for some $n \in \mathbb{Z}$ and $a_i \in \mathbb{C}$.

Hints:

1 What is the division algorithm?

3 ab What is the first isomorphism theorem? What is the Chinese remainder theorem? d Either use $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1)$ or consider the homomorphism $\mathbb{Z} \to R$ of Q2. efg Simplify by finding some $n \in \mathbb{N}$ in the ideal and first passing to the quotient by n. h Compare Q1.

4 First find an element in the kernel by inspection. Now use the division algorithm to show that the kernel is principal (note that $\mathbb{C}[x, y] = (\mathbb{C}[x])[y]$).

5 If $I = (f)$ where f is non-constant, consider the ideal $J = (f, p)$ for some prime p.

6 If θ is an automorphism of $\mathbb{Z}[x]$, what are the possibilities for $\theta(x)$?

7 Review the definitions of the direct product of rings and an ideal of a ring.

8 What is the pigeonhole principle?

9 What are the possibilities for the abelian group $(R, +)$?

10 Use the binomial theorem.

11 Use the binomial theorem.

12 Use Q2 and the universal property of the field of fractions.

13 a Recall that ideals of R/I correspond to ideals of R containing I. bc An element $a \in R$ is unit iff $(a) = R$.

14 a Explicitly determine the multiplicative inverse of an element $f \in \mathbb{C}[[x]]$ with nonzero constant term.