1 The Integers

Theorem 1.1 (Quotient-Remainder). *Let a and b be integers with $b \neq 0$. There exist unique integers q, r such that*

(1) $a = bq + r$, *and*

(2) $0 \leq r < |b|$.

Theorem 1.2 (GCD). *Let a and b be integers, at least one of them nonzero. The gcd of a and b is the smallest positive linear combination of a and b. In particular,* $\gcd(a, b) = au + bv$ *for some integers u and v.*

The set of all linear combinations of a and b equals the set of multiples of $\gcd(a, b)$.

Theorem 1.3 (Euclidean Algorithm). *The following algorithm produces* $\gcd(a, b)$.

```
def euclid_alg(a,b):
   if b == 0:
      print ("division by zero")
      return false
   else:
      r = a
      s = b
      while s != 0:
         rem =  r %s
         r = s
         s = rem
      return r
```

Theorem 1.4 (Prime-Irreducible). *An integer is irreducible if and only if it is prime.*

Theorem 1.5 (Unique Factorization). *Let a be a nonzero integer. There is*

- *a choice of $u = 1$ or -1,*
- *a nonnegative integer t,*
- *a set of positive prime numbers $p_1 < p_2 < \cdots < p_t$, and*
- *a set positive integers $e_1, \ldots, e_t$, such that*

$$a = up_1^{e_1} \cdots p_t^{e_t}$$

This factorization of a is uniquely determined.

2 The Univariate Polynomial Ring over a Field, K

Theorem 2.1 (Quotient-Remainder). *Let $a(x)$ and $b(x)$ be elements of $K[x]$ with $b(x) \neq 0$. There exist unique $q(x)$, $r(x)$ such that*

(1) $a(x) = b(x)q(x) + r(x)$, and

(2) $\deg r(x) < \deg b(x)$.

Theorem 2.2 (GCD). *Let $a(x), b(x) \in K[x]$ with at least one of them nonzero. There is a unique polynomial $d(x)$ satisfying*

(1) $d(x)$ is a common divisor of $a(x)$ and $b(x)$,

(2) $d(x)$ is monic,

(3) $d(x)$ is divisible by all other common divisors of $a(x)$ and $b(x)$ (so it is the greatest common divisor).

Furthermore, there exist $u(x), v(x) \in K[x]$ such that $d(x) = a(x)u(x) + b(x)v(x)$. The set of all polynomial combinations of $a(x)$ and $b(x)$ equals the set of multiples of $d(x)$.

Theorem 2.3 (Euclidean Algorithm). *The following algorithm produces* $\gcd(a, b)$.

```
def euclid_alg(a,b):
   if b == 0:
      print ("division by zero")
      return false
   else:
      r = a
      s = b
      while s != 0:
         rem =  r %s
         r = s
         s = rem
      return r
```

Theorem 2.4 (Prime-Irreducible). *Any nonconstant element of $K[x]$ is irreducible if and only if it is prime.*

Theorem 2.5 (Unique Factorization). *Let $a(x) \in K[x]$ be nonzero. There is a constant $u \in K$, a nonnegative integer t, distinct monic irreducible polynomials $p_1(x), \ldots, p_t(x)$, and positive integers $e_1, \ldots, e_t$ such that*

$$a(x) = u\big(p_1(x)\big)^{e_1} \cdots \big(p_t(x)\big)^{e_t}$$

Each of t, $p_i(x)$, e_i and u is uniquely determined, up to reordering of the $p_i(x)^{e_i}$.

3 Modular Computations (Quotient Rings)

Theorem 3.1 (Congruence modulo n)**.** *Congruence modulo n is an eqivalence relation. Furthermore, the set $\{0, 1, \ldots, n-1\}$ is a system of representatives for congruence modulo n in the sense that each integer a is congruent modulo n to exactly one element of $\{0, 1, \ldots, n-1\}$.*

Theorem 3.2 (Arithmetic modulo n)**.** *Suppose that $a \equiv b \bmod n$ and $r \equiv s \bmod n$. Then $a + r \equiv b + s \bmod n$ and $ar \equiv bs \bmod n$. Thus, arithmetic on congruence classes modulo n is well-defined as follows.*

- $[a] + [r] = [a + r]$
- $[a] * [r] = [ar]$

Theorem 3.3 (Congruence modulo $m(x)$)**.** *Congruence modulo $m(x)$ is an equivalence relation in $K[x]$. The set of polynomials of degree less than $\delta = \deg(m(x))$ is a system of representatives for congruence modulo $m(x)$. That is, each polynomial is congruent modulo $m(x)$ to its remainder when divided by $m(x)$. This remainder has degree less than δ.*

Theorem 3.4 (Arithmetic modulo $m(x)$)**.** *Suppose that $a(x) \equiv b(x) \bmod m(x)$ and $r(x) \equiv s(x) \bmod m(x)$. Then $a(x) + r(x) \equiv b(x) + s(x) \bmod m(x)$ and $a(x)r(x) = b(x)s(x) \bmod m(x)$. Thus, arithmetic on congruence classes modulo $m(x)$ is well-defined.*

- $[a(x)] + [r(x)] = [a(x) + r(x)]$
- $[a(x)] * [r(x)] = [a(x)r(x)]$

4 Problems

Problems 4.1. A QR theorem for $\mathbb{Z}[x]$ and for $\big(K[x]\big)[y]$?

(a) Under what conditions does the QR theorem work in these rings?

(b) When the QR theorem fails, how might you repair it?

Problems 4.2. Principal Ideal Domains (PIDs)

(a) Use induction and the GCD theorem to show that every finitely generated ideal in $\mathbb{Z}$ is principal.

(b) How can you show that every ideal in $\mathbb{Z}$ is principal?

(c) Treat the analogous questions for $K[x]$.

Problems 4.3. Primes and irreducibles more broadly

Let R be an integral domain (that is, it has no zero-divisors).

(a) Show that every prime element is irreducible.

Problems 4.4. Consequences of unique factorization

Prove these statements using the Unique Factorization theorem.

(a) Every nonzero rational number a can be uniquely expressed in the form

$$a = up_1^{e_1} \cdots p_t^{e_t}$$

for some $u = \pm 1$, $t \in \mathbb{N}_0$, prime numbers $p_1 < p_2 < \cdots < p_t$, and nonzero integers $e_1, \ldots, e_t$.

(b) Prove that any rational number can be expressed in a unique way in the form a/b with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ with $\gcd(a, b) = 1$. We call this expressing the rational number in **lowest terms**.

(c) Write analogous statements for $K(x)$.

Problems 4.5. Extending the greatest common divisor property to rational numbers.

This will be easier to do using unique factorization than just the GCD theorem. Let $\{a_1/b_1, \ldots, a_n/b_n\}$ be a set of rational numbers in lowest terms. Let $B = \operatorname{lcm}\{b_1, \ldots, b_n\}$ and $A = \gcd\{a_1, \ldots, a_n\}$.

(a) Show that $Ba_i/(Ab_i)$ is an integer for all $i = 1, \ldots, n$.

(b) Show that $\gcd\{Ba_1/(Ab_1), \ldots, Ba_n/(Ab_n)\} = 1$. [Suppose p is a prime dividing B, show there is some i such that p is not a factor of $Ba_i/(Ab_i)$.]

(c) Observe that the rational number A/B is similar to the GCD. If we factor it out of the rational numbers a_i/b_i we are left with a set of integers that have no common factor (other than 1).

Problems 4.6. Factorization Domains (FD) and Unique Factorization Domains (UFD)

For $R = K[x, y]$, define the total degree of $x^a y^b$ to be $a + b$ and the total degree of a polynomial to be the maximum of the total degree of its terms.

(a) Show that $\operatorname{TDeg}\big(a(x,y) * b(x,y)\big) = \operatorname{TDeg}\big(a(x,y)\big) + \operatorname{TDeg}\big(b(x,y)\big)$

(b) Use induction to show that $K[x, y]$ is an FD.