1 Finite Fields

Theorem 1.1. *Let K be a field with a finite number of elements.*

(1) K has p^n elements for some prime p and $n \in \mathbb{N}$.
(2) Each element of K is a root of $x^{p^n} - x$, so $x^{p^n} - x$ factors completely, into distinct linear factors, over K.
(3) There is an element $\eta \in K$ whose powers $\eta^1, \eta^2, \ldots, \eta^{p^n-1} = 1$ give all the nonzero elements of K. Consequently, K^* is cyclic of order $p^n - 1$.
(4) K is isomorphic to $\mathbb{F}_p[x]/m(x)$ for some irreducible polynomial $m(x)$ of degree n over $\mathbb{F}_p$. Furthermore $m(x)$ is a factor of $x^{p^n} - x$.

For any prime p and any positive integer n:

(5) There exists a field with p^n elements.
(6) Any two fields with p^n elements are isomorphic.
(7) The field with p^n elements has a subfield with p^d elements if and only if d divides n.

We use $\mathbb{F}_{p^n}$ to denote the unique field with p^n elements.

Proposition 1.2. *The field $\mathbb{F}_{p^d}$ is contained in $\mathbb{F}_{p^n}$ if and only if d divides n.*

2 Function Fields

(1) Starting with the polynomial ring $K[t]$ we can form a field, by creating the ring of fractions $D^{-1}k[t]$ where $D = K[t] \setminus \{0\}$. This is just

$$K(t) = \left\{ \frac{a(t)}{b(t)} : a(t), b(t) \in K[t], \text{ and } b(t) \neq 0 \right\}$$

(2) We can form new fields by taking the polynomial ring $\big(K(t)\big)[y]$ and modding out by an irreducible polynomial.

3 Rings and Algebras

Definition 3.1. A **ring** is a set R, with two operations $+$ and $*$ that satisfy the following properties.

(1) $+$ and $*$ are both commutative and associative.
(2) $+$ and $*$ both have identity elements (0 and 1 respectively).
(3) $+$ admits inverses $a + (-a) = 0$.
(4) $*$ distributes over $+$. That is $a * (b + c) = a * b + a * c$.

Strictly speaking, this defines a **commutative ring with identity**, but we refer to it simply as a ring.

Definition 3.2. Let R, S be rings. A function $\varphi : R \longrightarrow S$ is a *ring homomorphism* when the following hold:

(1) φ is a homomorphism of the additive groups $R, +_R$ and $S, +_S$. By theorem this is equivalent to
$$\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$$
(2) $\varphi(1_R) = 1_S$.
(3) For $r_1, r_2 \in R$,
$$\varphi(r_1 *_R r_2) = \varphi(r_1) *_S \varphi(r_2).$$

The universal homomorphism for $\mathbb{Z}$:

Theorem 3.3 (The Initial Ring)**.** *For any ring R there is a unique homomorphism from $\mathbb{Z}$ to R. The kernel is the set of multiples of some integer m. If $m = 0$ then R has a subring isomorphic to $\mathbb{Z}$. If $m > 0$, then R contains a subring isomorphic to $\mathbb{Z}/m$.*

We are interested in rings that all contain some particular field, K, which leads us to the following definition. (It can be generalized to an arbitrary ring K, but we won't need that.)

Definition 3.4. Let K be a field. A K**-algebra** (or algebra over K) is a ring R that contains K. Let R and S both be K-algebras. A K-algebra homomorphism $R \xrightarrow{\varphi} S$ is a ring homomorphism that satisfies $\varphi(a) = a$ for all $a \in K$.

We will always (ok, maybe there will be some exceptions) be dealing with K-algebras and homomorphisms of K-algebras in this course.

There is a universal property for a polynomial ring over K.

Theorem 3.5 (Universal property of polynomial rings). *Let R be a K-algebra. For any $r \in R$ there is a unique (K-algebra) homomorphism from $K[x]$ to R that takes x to r.*

$$\begin{aligned} \overline{\varphi} : K[x] &\longrightarrow R \\ \sum_i a_i x^i &\longmapsto \sum_i a_i s^i \end{aligned}$$

We will be dealing with K-algebras (basically polynomial rings $K[x_1, \ldots, x_n]$ and K-algebras rings derived from them, such as quotients rings). The main issue is that we will never (ok, perhaps with exceptions) deal with automorphims of K.

4 Ideals and Quotient Rings

Definition 4.1. An **ideal** of a ring R is a nonempty subset $I \subseteq R$ which is closed under addition and closed under multiplication by an arbitrary element of R:

(1) For $a, b \in I$, the sum $a + b$ must be an element of I.

(2) For $a \in I$ and any $r \in R$ the product ra must be an element of I.

We will say that I **absorbs products**.

The GCD theorem for $\mathbb{Z}$ may be interpreted as saying that the ideal generated by integers a, b is equal to the ideal generated by $\gcd(a, b)$. (A similar statement can be made for $K[x]$). The next proposition identifies the ideals we will be dealing with (and leaves open the question of infinitely generated ideals).

Proposition 4.2. *Let R be a ring.*

If an ideal I of R contains a unit, then $I = R$.

For any $a_1, a_2, \ldots, a_n \in R$, the following set is an ideal of R, and is called the ideal **generated by** $\{a_1, \ldots, a_n\}$.

$$I = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n : r_i \in R\}$$

The interest in ideals is that we can form quotient rings, as we did with $\mathbb{Z}/n$ and $K[x]/m(x)$.

Proposition 4.3. *Let R be a ring and let I be a proper ideal in R (that is $I \neq R$). Let $R/I = \{r + I : r \in R\}$. Then R/I is a ring, with additive structure defined by R/I as the quotient of the abelian group R by its subgroup I, and multiplicative structure defined by*

$$(r + I)(s + I) = rs + I$$

The additive identity is $0 + I$ and the multiplicative identity is $1 + I$.

The function $R \longrightarrow R/I$ that takes r to $r + I$ is a homomorphism of rings.

5 Properties of Elements and Ideals; Particular Types of Rings

There are particular types of elements, and particular types of rings that interest us.

Definition 5.1. An element u of a ring R is a **unit** when there is another element v such that $u * v = 1$. An element a of a ring R is a **zero-divisor** when $a \neq 0$ and there is some $b \neq 0$ in R such that $a * b = 0$. An element a of a ring R is **nilpotent** when there exists some positive integer n such that $a^n = 0$.

Definition 5.2. A **field** is a nontrivial ring in which every nonzero element is a unit. An **integral domain** is a nontrivial ring that has no zero-divisors. A nontrivial ring is **reduced** if it has no nilpotent elements other than 0.

Definition 5.3. Let I be a proper ideal of R (that is $I \neq R$). An ideal I is **maximal** if the only ideal properly containing I is R. The ideal I is **prime** when $ab \in I$ implies that either $a \in I$ or $b \in I$. The ideal I is **radical** when $a^n \in I$ for $n \in \mathbb{N}$ implies $a \in I$.

Theorem 5.4. *All prime ideals are radical. All maximal ideals are prime. Consequently, for a ring R*

$$\{\textit{maximal ideals in } R\} \subseteq \{\textit{prime ideals in } R\} \subseteq \{\textit{radical ideals in } R\}$$

Theorem 5.5. *Let R be a ring and I and ideal in R.*

(1) I is a maximal ideal if and only if R/I is a field.
(2) I is a prime ideal if and only if R/I is an integral domain.
(3) I is a radical ideal if and only if R/I is reduced.

Every field is an integral domain. Every integral domain is a reduced ring.

6 Problems

Problems 6.1. An algebraic extension of $K(t)$.

Consider the polynomial $y^3 - t^2 - t$ in $K(t)[y]$.

(a) Show that it is irreducible. Note: if it factors, it must have a root.

(1) Show that no element of $K[t]$ is a root by using unique factorization.

(2) Show that no element of $K(t)$ that is not a polynomial could possibly be a root by using lowest terms.

(b) Let $s = y + \langle y^3 - t^2 - t \rangle$, so that we can think of the field $K(t)[y]/\langle y^3 - t^2 - t \rangle$ as $K(t, s)$.

(1) Write down the general form of an element of $K(t, s)$.

(2) Find the inverse of s. [Multiply s by a general element and set equal to 1.]

(3) Show that the inverse of $s - 1$ is $\dfrac{1}{t^2 + t - 1}(s^2 + s + 1)$.

Problems 6.2. Playing with $\overline{\mathbb{F}}_p$.

Let $a(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ be an element of $\overline{\mathbb{F}}_p[x]$. Each coefficient is in some finite field, let us assume that $a_i \in \mathbb{F}_{p^{m_i}}$ but is in no smaller field.

(a) What is the smallest field containing all the coefficients?

(b) Suppose that $a(x)$ is irreducible in the field from part (a). What is the smallest field containing all of the roots of $a(x)$?

(c) [hard, mainly for discussion] Suppose $a(x)$ is not irreducible. What is the smallest field containing all of the roots of $a(x)$? Treat this for $n = \deg(a(x))$ equal to $2, 3, 4, 5, 6$ and consider the possible ways that $a(x)$ might factor.

Problems 6.3. K-algebras and product rings.

Let $R_1, R_2, \ldots, R_n$ be K-algebras.

(a) Show that $R_1 \times R_2 \times \cdots \times R_n$ is also a K-algebra. Identify the subring K in $R_1 \times R_2 \times \cdots \times R_n$.

(b) Identify the units in $R_1 \times R_2 \times \cdots \times R_n$.

(c) Identify the nilpotents in $R_1 \times R_2 \times \cdots \times R_n$.

(d) Identify the zero-divisors in $R_1 \times R_2 \times \cdots \times R_n$.

Problems 6.4. The universal property of $K[x]$.

(a) Let $a \in K$ and consider the homomorphism from $K[x]$ to K that takes x to a. What is the kernel of this homomorphism?

(b) Let $a_1, \ldots, a_n \in K$ and consider the homomorphism from $K[x]$ to the ring K^n that takes x to $(a_1, a_2, \ldots, a_n)$. What is the kernel of this homomorphism?

(c) Let $g(x) \in K[x]$ and consider the homomorphism from $K[x]$ to $K[x]$ x to $g(x)$.

(1) What is the kernel of this homomorphism?

(2) Under what conditions is this map an isomorphism?

Problems 6.5.

(a)

Problems 6.6.

(a)