# Algebra Review 2

## 1 Fields

A field is an extension of the concept of a group.

**Definition 1.** A *field* $(F, +, \cdot, 0_F, 1_F)$ is a set $F$ together with two binary operations $(+, \cdot)$ on $F$ such that the following conditions hold:

1. $(F, +)$ is a commutative group, with identity the element $0_F$.
2. The $\cdot$ operation is associative, i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c, \in F$.
3. The $\cdot$ operation is commutative, i.e., $a \cdot b = b \cdot a$ for all $a, b \in F$.
4. The distributive law holds, i.e., $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in F$.
5. The element $1_F$ is an identity for $\cdot$, i.e., $1_F \cdot a = a \cdot 1_F = a$ for all $a \in F$.
6. All nonzero element in $F$ have an inverse under $\cdot$, i.e., for all $a \in F, a \neq 0_F$, there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1_F$. □

**Example 2.** $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field. □

**Example 3.** The set $\mathbb{Z}_5$ is a field, under addition and multiplication modulo 5. To see this, we already know that $\mathbb{Z}_5$ is a group under addition. Furthermore, we can easily check that requirements $2 - 5$ are satisfied. The non-trivial one to check is condition 6, but this can be verified on a case-by-case basis (i.e., the inverse of 2 is 3; 4 is its own inverse).

However, the set $\mathbb{Z}_6$ is not a field, because the element 4 has no multiplicative inverse (try to find one!). □

**Theorem 4.** $\mathbb{Z}_p$ is a field under addition and multiplication modulo $p$ if and only if $p$ is prime. □

**Remark 5.** Some notations:

1. We sometimes abuse notation by writing 0 (resp. 1) instead of $0_F$ (resp. $1_F$) when explicit from the context.
2. We sometimes use $ab$ instead of $a \cdot b$.
3. Subtraction $a - b$ is defined by $a + (-b)$, and division $a/b$ by $ab^{-1}$ for $b \neq 0_F$.
4. We denote $\overbrace{a + \cdots + a}^{m \text{ times}}$ by $ma$ for $m \in \mathbb{N}$, and also $\overbrace{a \cdot \cdots \cdot a}^{m \text{ times}}$ by $a^m$. When we write $-ma$ it means $m(-a)$, and $a^{-m}$ means $(a^{-1})^m$.
5. The value $a^0$ is defined to be $1_F$, and $0a$ to be $0_F$. □

**Lemma 6.** Let $F$ be a field. Then, for all $a \in F$, and $n_1, n_2 \in \mathbb{Z}$,

$$(a^{n_1})^{n_2} = a^{n_1 n_2} \quad a^{n_1} a^{n_2} = a^{n_1+n_2} \ .$$

□

**Lemma 7.** Let $F$ be a field. If the elements $a, b \in F$ are such that $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

*Proof.* Suppose towards contradiction that $ab = 0$. If $a \neq 0$ then $a$ has inverse. So we have

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1} \cdot a)b = 1 \cdot b = b \ \text{ (contradiction)}.$$

By symmetry, if $b \neq 0$, then we have $a = 0$ (contradiction). □

When, however, $F$ is not a field the above lemma no more holds. Consider $4 \cdot 3$ in $\mathbb{Z}_6$.

### 1.1 Finding a multiplicative inverse in $\mathbb{Z}_p^*$

As we saw in class, we often need the inverse of a number in $\mathbb{Z}_p^*$ . Therefore, it is essential to have an efficient algorithm to find the inverse.

---

**Algorithm 1** Calcuate $a^{-1} \mod p$.

---

**Input:** $(a, p)$
**Output:** $a^{-1} \mod p$

Compute $x$ and $y$ s.t.

$$ax + py = 1 \ .$$

This can be efficiently computed because $\gcd(a, p) = 1$. See Problem Set 1 for the details.
**return** $x \mod p$.

---

## 2 Polynomials

**Definition 8.** If $F$ is a field, then a *polynomial* in the indeterminate (or formal variable) $x$ over the field $F$ is an expression of the form

$$f(x) = a_n x^n + \cdots + a_1 x_1 + a_0$$

where each $a_i \in F$ and $n \geq 0$.

- The element $a_i$ is called the *coefficient* of $x^i$ in $f(x)$.
- The largest integer $m$ which $a_m \neq 0$ is called the *degree* of $f(x)$, denoted $\mathsf{deg}(f(x))$.
- The element $a_m$ for $m = \mathsf{deg}(f(x))$ is called the *leading coefficient* of $f(x)$.
- If $f(x) = a_0$ (a *constant polynomial*) and $a_0 \neq 0$, then $\mathsf{deg}(f(x))$ is 0.

- If all the coefficients of $f(x)$ are 0, then $f(x)$ is called the *zero polynomial*, and $\mathsf{deg}(f(x)) = -\infty$.

- The polynomial $f(x)$ is said to be *monic* if the leading coefficient is 1. $\square$

Now we will define addition and multiplication of polynomials. For technical convenience, we will write polynomials as an infinite sum $\sum_{i=0}^{\infty} a_i x^i$ with only finite number of the coefficients being non-zero.

**Definition 9.** Given the two polynomials

$$f(x) = \sum_{i=0}^{\infty} a_i x^i \quad \text{and} \quad g(x) = \sum_{i=0}^{\infty} b_i x_i \ ,$$

the *addition* of $f(x)$ and $g(x)$ is defined as

$$f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i \ ,$$

and the *multiplication* of $f(x)$ and $g(x)$ is defined as

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} \left( \sum_{j=0}^{i} a_j b_{i-j} \right) x^i \ .$$

$\square$

**Definition 10.** Let $F$ be a field. The *polynomial ring* $F[x]$ is the ring formed by the set of all polynomials in the indeterminate $x$ having coefficient from $F$. The two operations are the polynomial addition and multiplication with coefficient arithmetic performed in the field $F$. $\square$

The set $(R, +, \cdot, 0_R, 1_R)$ is called the *ring* when all the requirements of the Definition 1 except the 6-th item are satisfied. It is easy to see $F[x]$ is a ring.

**Note 11.** The indeterminate $x$ in a polynomial $f(x) \in F[x]$ is *not an element of the field $F$*. It is just a "formal" variable. So we must not treat $f(x)$ as just a polynomial function. In particular, two polynomials are equal if and only if their coefficients are equal.

**Example 12.** Consider the polynomials $a(x) = x^2 + 3$, $b(x) = 4x^3 + 2x + 1$, $c(x) = 5 = 0$, $d(x) = 1 + x$, $e(x) = x$, and $f(x) = 4x^3$ in $\mathbb{Z}_5[x]$. Then We have

$a(x)+b(x) = 4x^3+x^2+2x+4$, $a(x)\cdot b(x) = 4x^5+4x^3+x^2+x+3$, $c(x)\cdot d(x)+e(x)\cdot f(x) = 4x^4$. $\square$

**Lemma 13.** Let $f(x)$ and $g(x)$ be polynomials in $F[x]$ for a field $F$. Then, we have

$$\mathsf{deg}(f(x) + g(x)) \le \max\left(\mathsf{deg}(f(x)), \mathsf{deg}(g(x))\right)$$
$$\mathsf{deg}(f(x) \cdot g(x)) = \mathsf{deg}(f(x)) + \mathsf{deg}(g(x))$$

□

**Theorem 14.** If $f(x), h(x) \in F[x]$ with $h(x) \neq 0$, then polynomial division of $f(x)$ by $h(x)$ yields polynomial $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)h(x) + r(x), \quad \text{where } \mathsf{deg}(r(x)) < \mathsf{deg}(h(x)).$$

Moreover, $q(x)$ and $r(x)$ are unique. □

**Definition 15.** Let $f(x)$ and $h(x)$ be polynomials in $F[x]$ for a field $F$. $h(x)$ *divides* $f(x)$, and we write $h(x)|f(x)$, if there exists a polynomial $q(x) \in F[x]$ such that $f(x) = q(x)h(x)$. □

**Definition 16.** For a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ and an element $\alpha \in F$, the *evaluation* of $f(x)$ at $\alpha$ (or *substituting* $\alpha$ for $x$ in $f(x)$) is $f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0$. Evaluation is also denoted by $f|_{x=a}$. □

Note in the above definition that now we can do actual additions and multiplications in $F$, since $\alpha \in F$. We have of course $f(\alpha) \in F$. Also, we can see for any $f, g \in F[x], \alpha \in F$

$$(f+g)(\alpha) = f(\alpha) + g(\alpha) \;\text{ and }\; (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)\ .$$

**Definition 17.** Let $F$ be a field. An element $\alpha \in F$ is called a *root* of $f(x) \in F[x]$ if $f(\alpha) = 0$. □

**Lemma 18.** Let $F$ be a field. For $f(x) \in F[x]$ and $\alpha \in F$, we have $f(x) = (x-\alpha)q(x) + f(\alpha)$.

*Proof.* By Theorem 14, there exist unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = (x-\alpha)q(x) + r(x) \quad \text{with } \mathsf{deg}(r(x)) < \mathsf{deg}(x-a) = 1\ .$$

So, $r(x)$ must be a constant $\beta \in F$. We find the exact value of $\beta$ by substituting $\alpha$ for $x$:

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + \beta = 0 + \beta = \beta.$$

□

**Corollary 19.** Let $F$ be a field. For $f(x) \in F[x]$ and $\alpha \in F$, $(x-\alpha)$ divides $f(x)$, if and only if $\alpha$ is a *root* of $f(x)$ □

**Example 20.** Consider the polynomials $f_1(x) = x^6 + x^5 + x^3 + x^2 + x + 1$, $f_2(x) = x^5 + x^3 + x + 1$, and $h(x) = x^4 + x^3 + 1$ in $\mathbb{Z}_2[x]$. Then, the divisions yield

$$f_1(x) = x^2 h(x) + (x^3 + x + 1) \quad \text{and} \quad f_2(x) = (x+1)h(x).$$

Therefore, $h(x)$ divides $f_2(x)$. The evaluations are: $f_1(0) = 1, f_1(1) = 0, f_2(0) = 1, f_2(1) = 0$. The element 1 is a root of $f_1$ and $f_2$. □

**Theorem 21.** Let $f(x)$ be a nonzero polynomial in $F[x]$ of degree $d$ for a field $F$. Then $f(x)$ has at most $d$ distinct roots in $F$.

*Proof.* The proof proceeds by induction on $d$. The result is clearly true for $d = 0$. For $d = 1$, the polynomial will of the following form: $ax + b = a(x + b/a)$, whose unique root is $-b/a$. Assume now that $d > 1$ and that this theorem holds for all polynomials of degree less than $d$. Consider a polynomial $f(x)$ of degree $d$. Let $\alpha$ be a root (if there is no root, then we are done). Then we have

$$f(x) = (x - \alpha)q(x).$$

The degree of $q(x)$ is $d - 1$ (by Lemma 13). Suppose we have another root $\gamma \neq \alpha$. Then we have

$$f(\gamma) = (\alpha - \gamma)q(\gamma).$$

Since $(\alpha - \gamma) \neq 0$, $q(\gamma)$ must be 0 (by Lemma 7). This means all the roots of $f$ other than $\alpha$ are also the roots of $q$. Because, by induction, $q$ has at most $d - 1$ distinct roots, $f(x)$ has $1 + (d - 1) = d$ distinct roots. $\square$