20241215 MATH3301 NOTE 9[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Introduction

This note intends to connect fields with polynomials.

2 Polynomial Ring $R[t]$

2.1 Convolution

Definition 2.1. (**Convolution**)
Let R be a nonzero commutative ring.
Define convolution $*$ on the set of all R-valued sequences by:

$$a * b[n] = \sum_{i+j=n} a_i b_j$$

Lemma 2.2. Convolution is commutative.

Proof. For all R-valued sequences a, b:

$$a * b[n] = \sum_{i+j=n} a_i b_j = \sum_{j+i=n} b_j a_i = b * a[n]$$

Quod. Erat. Demonstrandum. □

Lemma 2.3. Convolution is associative.

Proof. For all R-valued sequences a, b, c:

$$(a * b) * c[n] = \sum_{i+j+k=n} a_i b_j c_k = a * (b * c)[n]$$

Quod. Erat. Demonstrandum. □

Lemma 2.4. If R has a unity 1, then $*$ has an identity $1 = (1, 0, 0, \cdots)$.

Proof. For all R-valued sequence a:

$$1 * a[n] = \sum_{i+j=n} \delta_{0,i} a_j = a_n$$

Quod. Erat. Demonstrandum. □

Lemma 2.5. If R has unity 1 and $a_0 b_0 = 1$, then $(a_0, 0, 0, \cdots) * (b_0, 0, 0, \cdots) = 1$.

Proof.

$$a * b[n] = \sum_{i+j=n} a_i b_j = a_0 b_0 \sum_{i+j=n} \delta_{0,i}\delta_{0,j} = \delta_{0,n}$$

Quod. Erat. Demonstrandum. □

Example 2.6. In $\mathbb{Z}_4$, if $a_n = \delta_{0,n} + 2\delta_{1,n}$, then $a^2 = 1$. Hence, all invertible element a under $*$ are not necessarily given by **Lemma 2.5.**.

Lemma 2.7. Convolution distributes over addition.

Proof. For all R-valued sequences λ, a, b:

$$\lambda * (a+b)[n] = \sum_{i+j=n} \lambda_i(a_j + b_j) = \sum_{i+j=n} \lambda_i a_j + \sum_{i+j=n} \lambda_i b_j = \lambda * a + \lambda * b[n]$$

Quod. Erat. Demonstrandum. □

Definition 2.8. (**The Formal Power Series Ring** $R[\![t]\!]$)
Let R be a nonzero commutative ring. If we define an indeterminate $t = (0, 1, 0, \cdots)$ in the set $R[\![t]\!]$ of all R-valued sequences, and identify all expressions $a_0 + a_1 t + a_2 t^2 + \cdots$ with $(a_0, a_1, a_2, \cdots)$, then $R[\![t]\!]$ forms a commutative ring, namely, the formal power series ring, under $+$ and $*$.

Remark: *The elements of $R[\![t]\!]$ are called formal power series. We denote them by $f(t), g(t), h(t), \cdots$. If there is no ambiguity, we write them as $f, g, h, \cdots$, and omit $*$.*

Example 2.9. As every integer n in $R[\![t]\!]$ is a constant, $\mathrm{Char}(R[\![t]\!]) = \mathrm{Char}(R)$.

Theorem 2.10. $R[\![t]\!]$ has a zero divisor iff R has a zero divisor.

Proof. We may divide our proof into two parts.
"if" direction: If the product of some nonzero elements s, t of R is 0,
then the product of some nonzero elements $a = s, b = t$ of $R[\![t]\!]$ is 0.
"only if" direction: If the product of some nonzero elements a, b of $R[\![t]\!]$ is 0,
then take the minimal nonzero entries $s = a_i, t = b_j$ of a, b respectively,
the product of some nonzero elements s, t of R is $a_i b_j = a * b[i+j] = 0$.
Hence, we've proven the logical equivalence. Quod. Erat. Demonstrandum. □

Example 2.11. As the product of $t, f(t)$ has no constant term, t is not a unit.

Example 2.12. In $\mathbb{Z}[\![t]\!]$, the ideal $\langle 2, t\rangle$ is not principal, because for all $f(t) \in \mathbb{Z}[\![t]\!]$, either the constant term of $f(t)$ is even, and $\langle f(t)\rangle$ misses t, or the constant term of $f(t)$ is odd, and $\langle f(t)\rangle$ misses 2. In both cases, $\langle f(t)\rangle \neq \langle 2, t\rangle$.

Theorem 2.13. (**The Polynomial Ring** $R[t]$)
Let R be a nonzero commutative ring.
The following subset $R[t]$, namely, the polynomial ring, forms a subring of $R[\![t]\!]$:

$$R[t] = \{a(t) \in R[\![t]\!] : \exists M \geq 0, \forall i \geq M, a_i = 0\}$$

Proof. We may divide our proof into four parts.
Part 1: $\exists 0 \geq 0, \forall i \geq 0, 0 = 0$, so $0 \in R[t]$.
Part 2: For all $a(t), b(t) \in R[\![t]\!]$:

$$\begin{aligned} a(t), b(t) \in R[t] &\implies \exists M \geq 0, \forall i \geq M, a_i = 0 \text{ and } \exists N \geq 0, \forall j \geq N, b_j = 0 \\ &\implies \exists \mathrm{Max}\{M, N\} \geq 0, \forall k \geq \mathrm{Max}\{M, N\}, a_k + b_k = 0 + 0 = 0 \\ &\implies a(t) + b(t) \in R[t] \end{aligned}$$

Part 3: For all $a(t) \in R[\![t]\!]$:

$$\begin{aligned} a(t) \in R[t] &\implies \exists M \geq 0, \forall i \geq M, a_i = 0 \\ &\implies \exists M \geq 0, \forall i \geq M, -a_i = -0 = 0 \\ &\implies -a(t) \in R[t] \end{aligned}$$

Part 4: For all $a(t), b(t) \in R[\![t]\!]$:

$$\begin{aligned} a(t), b(t) \in R[t] &\implies \exists M \geq 0, \forall i \geq M, a_i = 0 \text{ and } \exists N \geq 0, \forall j \geq N, b_j = 0 \\ &\implies \exists M + N \geq 0, \forall k \geq M + N, \sum_{i+j=k} a_i b_j = \sum_{i+j=k} 0 = 0 \\ &\implies a(t)b(t) \in R[t] \end{aligned}$$

$R[t]$ contains unity if R does. Quod. Erat. Demonstrandum. $\square$

2.2 The Evaluation Ring Homomorphism

Theorem 2.14. (**The Evaluation Ring Homomorphism**)
Let R, S be two nonzero commutative rings, s be an element of S, and $\phi : R \to S$ be a ring homomorphism. The following map σ_s is a ring homomorphism:

$$\sigma_s : R[t] \to S, \sigma_s\left(\sum_{i=0}^{+\infty} a_i t^i\right) = \sum_{i=0}^{+\infty} \phi(a_i) s^i$$

Proof. We may divide our proof into four parts.
Part 1: As $\exists M \geq 0, \forall i \geq M, a_i = 0$, the summation $\sum_{i=0}^{+\infty} \phi(a_i)s^i$ contains finitely many nonzero terms, thus σ_s is well-defined.
Part 2: For all $\sum_{i=0}^{+\infty} a_i t^i, \sum_{j=0}^{+\infty} b_j t^j \in R[t]$:

$$\begin{aligned}\sigma_s\left(\sum_{i=0}^{+\infty} a_i t^i + \sum_{j=0}^{+\infty} b_j t^j\right) &= \sigma_s\left(\sum_{k=0}^{+\infty}(a_k + b_k)t^k\right) = \sum_{k=0}^{+\infty}\phi(a_k + b_k)s^k \\ &= \sum_{k=0}^{+\infty}(\phi(a_k) + \phi(b_k))s^k = \sum_{i=0}^{+\infty}\phi(a_i)s^i + \sum_{j=0}^{+\infty}\phi(b_j)s^j \\ &= \sigma_s\left(\sum_{i=0}^{+\infty} a_i t^i\right) + \sigma_s\left(\sum_{j=0}^{+\infty} b_j t^j\right)\end{aligned}$$

Part 3: For all $(a_0, a_1, a_2, \cdots), (b_0, b_1, b_2, \cdots) \in R[t]$:

$$\begin{aligned}\sigma_s\left(\sum_{i=0}^{+\infty} a_i t^i \sum_{j=0}^{+\infty} b_j t^j\right) &= \sigma_s\left(\sum_{k=0}^{+\infty}\sum_{i+j=k} a_i b_j t^k\right) = \sum_{k=0}^{+\infty}\phi\left(\sum_{i+j=k} a_i b_j\right)s^k \\ &= \sum_{k=0}^{+\infty}\sum_{i+j=k}\phi(a_i)\phi(b_j)s^k = \sum_{i=0}^{+\infty}\phi(a_i)s^i\sum_{j=0}^{+\infty}\phi(b_j)s^j \\ &= \sigma_s\left(\sum_{i=0}^{+\infty} a_i t^i\right)\sigma_s\left(\sum_{j=0}^{+\infty} b_j t^j\right)\end{aligned}$$

σ_s preserves unity if R, S have. Quod. Erat. Demonstrandum. $\square$

Definition 2.15. (**Circulant Matrix**)
Let R be a nonzero commutative ring.
Define circulant matrix as a matrix in the following form:

$$C = \begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_3 & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & \cdots & c_4 & c_3 & c_2 \\ c_2 & c_1 & c_0 & \cdots & c_5 & c_4 & c_3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ c_{n-3} & c_{n-4} & c_{n-5} & \cdots & c_0 & c_{n-1} & c_{n-2} \\ c_{n-2} & c_{n-3} & c_{n-4} & \cdots & c_1 & c_0 & c_{n-1} \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_2 & c_1 & c_0 \end{pmatrix}$$

We collect all n by n R-valued circulant matrices in the set $\mathbf{C}_n(R)$.

Example 2.16. Let R be a nonzero commutative ring with unity.
If we define the following circulant matrix:

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

And define a ring homomorphism $\phi : R \to \mathbf{C}_n(R), r \mapsto rI$,
then the evaluation ring homomorphism $\sigma_H : R[t] \to S$ is explicitly given by:

$$\sigma_H\left(\sum_{i=0}^{+\infty} a_i t^i\right) = \sum_{k=0}^{n-1}\sum_{i=0}^{+\infty} a_{6i+k} H^k$$

3 Polynomial Ring $F[t]$

3.1 Division Algorithm

Definition 3.1. (**Degree Function** Deg)
Let F be a field. Define degree function $\mathrm{Deg} : F[t] \to \{-\infty\} \cup \mathbb{Z}_{\geq 0}$ by:

$$\mathrm{Deg}(f(t)) = \begin{cases} -\infty & \text{if} \quad f(t) = 0; \\ [\text{The minimal } i \geq 0 \text{ such that } a_i \neq 0] & \text{if} \quad f(t) \neq 0; \end{cases}$$

Remark: *According to well-ordering principle,* Deg *is well-defined.*

Proposition 3.2. Let F be a field, and $f(t), g(t)$ be two polynomials in $F[t]$.
(1) $\mathrm{Deg}(f(t) + g(t)) \leq \mathrm{Max}\{\mathrm{Deg}(f(t)), \mathrm{Deg}(g(t))\}$.
(2) $\mathrm{Deg}(f(t)g(t)) = \mathrm{Deg}(f(t)) + \mathrm{Deg}(g(t))$.

Proof. We may divide our proof into two cases.
Case 1: If $f(t) = 0$ or $g(t) = 0$, then we may assume $f(t) = 0$:

$$\begin{aligned} \mathrm{Deg}(f(t) + g(t)) &= \mathrm{Deg}(0 + g(t)) = \mathrm{Deg}(g(t)) = \mathrm{Max}\{-\infty, \mathrm{Deg}(g(t))\} \\ &= \mathrm{Max}\{\mathrm{Deg}(0), \mathrm{Deg}(g(t))\} = \mathrm{Max}\{\mathrm{Deg}(f(t)), \mathrm{Deg}(g(t))\} \\ \mathrm{Deg}(f(t)g(t)) &= \mathrm{Deg}(0g(t)) = \mathrm{Deg}(0) = -\infty = -\infty + \mathrm{Deg}(g(t)) \\ &= \mathrm{Deg}(0) + \mathrm{Deg}(g(t)) = \mathrm{Deg}(f(t)) + \mathrm{Deg}(g(t)) \end{aligned}$$

Case 2: If $f(t) \neq 0$ and $g(t) \neq 0$, then:

$$\begin{aligned}
\mathrm{Deg}(f(t)) = i \text{ and } \mathrm{Deg}(g(t)) = j &\implies f(t) \text{ has no term after } t^i \\
&\quad\text{and } g(t) \text{ has no term after } t^j \\
&\implies f(t)+g(t) \text{ has no term after } t^{\mathrm{Max}\{i,j\}} \\
&\implies \mathrm{Deg}(f(t)+g(t)) \leq \mathrm{Max}\{i,j\} \\
\mathrm{Deg}(f(t)) = i \text{ and } \mathrm{Deg}(g(t)) = j &\implies f(t) = \cdots + a_i t^i \text{ and } a_i \neq 0 \\
&\quad\text{and } g(t) = \cdots + b_j t^j \text{ and } b_j \neq 0 \\
&\implies f(t)g(t) = \cdots + a_i b_j t^{i+j} \text{ and } a_i b_j \neq 0 \\
&\implies \mathrm{Deg}(f(t)g(t)) = i + j
\end{aligned}$$

Quod. Erat. Demonstrandum. □

Example 3.3. Let R be a commutative ring, and $f(t), g(t)$ be two polynomials in $R[t]$. The property $\mathrm{Deg}(f(t)+g(t)) \leq \mathrm{Max}\{\mathrm{Deg}(f(t)), \mathrm{Deg}(g(t))\}$ still holds.

Example 3.4. In $\mathbb{Z}_4[t]$, if $f(t) = g(t) = 2$, then $f(t)g(t) = 0$.
The property $\mathrm{Deg}(f(t)g(t)) = \mathrm{Deg}(f(t)) + \mathrm{Deg}(g(t))$ is violated.

Theorem 3.5. (**Division Algorithm**)
Let F be a field, and $a(t), b(t)$ be two polynomials in $F[t]$.
If $b(t) \neq 0$, then for some unique $q(t), r(t) \in F[t]$:

$$a(t) = q(t)b(t) + r(t) \text{ and } \mathrm{Deg}(r(t)) < \mathrm{Deg}(b(t))$$

Proof. Assume that $\mathrm{Deg}(g(t)) = m \geq 0$, the uniqueness is clear as below:

$$\begin{aligned}
a(t) = q_1(t)b(t) + r_1(t) = q_2(t)b(t) + r_2(t) &\implies b(t) | r_2(t) - r_1(t) \\
&\implies q_1(t) = q_2(t) \text{ and } r_1(t) = r_2(t)
\end{aligned}$$

We prove the existence by mathematical induction.
(1) When $\mathrm{Deg}(a(t)) < \mathrm{Deg}(b(t))$, there exist $0, a(t) \in F[t]$, such that:

$$a(t) = 0b(t) + a(t) \text{ and } \mathrm{Deg}(a(t)) < \mathrm{Deg}(b(t))$$

(2) For all $n \geq \mathrm{Deg}(b(t))$, when $\mathrm{Deg}(a(t)) < n$, assume the existence of $q(t), r(t) \in F[t]$.
(3) When $\mathrm{Deg}(a(t)) = n$, $a(t) = \cdots + a_n t^n, b(t) = \cdots + b_m t^m$, where $a_n, b_m \neq 0$.
Define $A(t) = a(t) - \frac{a_n t^n}{b_m t^m} b(t)$, as $\mathrm{Deg}(A(t)) < n$,
we may apply the inductive hypothesis to find $Q(t), R(t) \in F[t]$, such that:

$$A(t) = Q(t)b(t) + R(t) \text{ and } \mathrm{Deg}(R(t)) < \mathrm{Deg}(b(t))$$

Now, for some $q(t) = Q(t) + \frac{a_n t^n}{b_m t^m}, r(t) = R(t) \in F[t]$:

$$a(t) = q(t)b(t) + r(t) \text{ and } \mathrm{Deg}(r(t)) < \mathrm{Deg}(b(t))$$

Hence, we've proven the existence. Quod. Erat. Demonstrandum. □

3.2 Principal Ideal Property

Definition 3.6. (**Greatest Common Divisor**)
Let F be a field, $(a_\lambda(t))_{\lambda \in I}$ be an indexed family in $F[t]$, and $b(t)$ be a polynomial in $F[t]$. If $b(t)$ is a common divisor of $(a_\lambda(t))_{\lambda \in I}$, and every common divisor of $(a_\lambda(t))_{\lambda \in I}$ divides $b(t)$, then $b(t)$ is a greatest common divisor of $(a_\lambda(t))_{\lambda \in I}$.

Definition 3.7. (**Least Common Multiple**)
Let F be a field, $(a_k(t))_{k=1}^m$ be a finite list in $F[t]$, and $b(t)$ be a polynomial in $F[t]$. If $b(t)$ is a common multiple of $(a_k(t))_{k=1}^m$, and $b(t)$ divides every common multiple of $(a_k(t))_{k=1}^m$, then $b(t)$ is a least common multiple of $(a_k(t))_{k=1}^m$.

Remark: *To prove the existence of greatest common divisor and least common multiple, we need to apply principal ideal property.*

Example 3.8. Let F be a field, $(a_k(t))_{k=1}^m$ be a nonempty finite list in $F[t]\backslash\{0\}$, $A(t) = \prod_{k=1}^m a_k(t)$ be their product, and $(A_k(t) = \prod_{l \neq k} a_l(t))_{k=1}^m$ be their dual. For all $b(t), B(t) \in F[t]$ with $b(t)B(t) = A(t)$, the followings are equivalent:
(1) $b(t)$ is a common multiple of $(a_k(t))_{k=1}^m$.
(2) $B(t)$ is a common divisor of $(A_k(t))_{k=1}^m$.
Hence, the followings are equivalent:
(1) $b(t)$ is a least common multiple of $(a_k(t))_{k=1}^m$.
(2) $B(t)$ is a greatest common divisor of $(A_k(t))_{k=1}^m$.

Example 3.9. In $\mathbb{Z}[\sqrt{5}\mathrm{i}]$, $6, 2+2\sqrt{5}\mathrm{i}$ have common divisors $\pm 1, \pm 2, \pm(1+\sqrt{5}\mathrm{i})$, where the maximal divisors $\pm 2, \pm(1+\sqrt{5}\mathrm{i})$ are not associated, so greatest common divisor of $6, 2+2\sqrt{5}\mathrm{i}$ fails to exist.[2]

Proposition 3.10. Let F be a field. $F[t]$ is a principal ideal domain.

Proof. As F is an integral domain, $F[t]$ is an integral domain.
For all nonzero ideal $\mathfrak{a}$ of $F[t]$, well-ordering principal suggests that $\mathfrak{a}$ contains a nontrivial element $b(t)$ where $\mathrm{Deg}(b(t))$ is minimal. Assume to the contrary that $b(t)$ doesn't divide some $a(t) \in \mathfrak{a}$. Apply division algorithm, and we get the remainder $r(t)$ of $a(t)$ modulo $b(t)$, which is a nontrivial element in $\mathfrak{a}$, and this contradicts with the minimality of $\mathrm{Deg}(b(t))$. Hence, $\mathfrak{a} = \langle a(t) \rangle$ is principal. Quod. Erat. Demonstrandum. □

Remark: *To keep principal ideal property, we construct polynomial ring over a field.*

Theorem 3.11. Let F be a field, $(a_\lambda(t))_{\lambda\in I}$ be a nonempty indexed family in $F[t]$, and $b(t)$ be a greatest common divisor of $(a_\lambda(t))_{\lambda\in I}$.

$$\sum_{\lambda\in I}\langle a_\lambda(t)\rangle = \langle b(t)\rangle$$

Proof. We may divide our proof into two parts.
"$\subseteq$ inclusion": For all $\lambda \in I$, $b(t)|a_\lambda(t)$ iff $\langle b(t)\rangle \supseteq \langle a_\lambda(t)\rangle$, so:

$$\sum_{\lambda\in I}\langle a_\lambda(t)\rangle \subseteq \langle b(t)\rangle$$

"$\supseteq$ inclusion": As $F[t]$ is a principal ideal domain, for some $B(t) \in F[t]$:

$$\sum_{\lambda\in I}\langle a_\lambda(t)\rangle = \langle B(t)\rangle$$

For all $\lambda \in I$, $\langle B(t)\rangle \supseteq \langle a_\lambda(t)\rangle$ iff $B(t)|a_\lambda(t)$, so:

$$B(t) \text{ is a common divisor of } (a_\lambda(t))_{\lambda\in I}$$

As $b(t)$ is greatest, $B(t)|b(t)$, and it follows that:

$$\sum_{\lambda\in I}\langle a_\lambda(t)\rangle \supseteq \langle b(t)\rangle$$

To conclude, we've proven the equality. Quod. Erat. Demonstrandum. □

Remark: *This simultaneously proves the existence of greatest common divisor.*

Theorem 3.12. Let F be a field, $(a_k(t))_{k=1}^m$ be a nonempty finite list in $F[t]$, and $b(t)$ be a least common multiple of $(a_k(t))_{k=1}^m$.

$$\bigcap_{k=1}^{m}\langle a_k(t)\rangle = \langle b(t)\rangle$$

Proof. We may divide our proof into two parts.
"$\supseteq$ inclusion": For all $1 \leq k \leq m$, $a_k(t)|b(t)$ iff $\langle a_k(t)\rangle \supseteq \langle b(t)\rangle$, so:

$$\bigcap_{k=1}^{m}\langle a_k(t)\rangle \supseteq \langle b(t)\rangle$$

"$\subseteq$ inclusion": As $F[t]$ is a principal ideal domain, for some $B(t) \in F[t]$:

$$\bigcap_{k=1}^{m}\langle a_k(t)\rangle = \langle B(t)\rangle$$

For all $1 \leq k \leq m$, $\langle a_\lambda(t) \rangle \supseteq \langle B(t) \rangle$ iff $a_k(t) | B(t)$, so:

$$B(t) \text{ is a common multiple of } (a_k(t))_{k=1}^m$$

As $b(t)$ is least, $b(t)|B(t)$, and it follows that:

$$\bigcap_{k=1}^m \langle a_k(t) \rangle \subseteq \langle b(t) \rangle$$

To conclude, we've proven the equality. Quod. Erat. Demonstrandum. ☐

Remark: *This simultaneously proves the existence of least common multiple.*

3.3 Root and Irreducibility

Definition 3.13. (**Maximal Ideal**)
Let R be a commutative ring with unity, and $\mathfrak{p}$ be a proper ideal of R.
If $\forall a \in \mathfrak{p}^c, \langle a \rangle + \mathfrak{p} = R$, then $\mathfrak{p}$ is maximal.

Definition 3.14. (**Prime Ideal**)
Let R be a commutative ring with unity, and $\mathfrak{p}$ be a proper ideal of R.
If $\forall \mathfrak{p}^c \ni a, \forall \mathfrak{p}^c \ni b, \mathfrak{p}^c \ni ab$, then $\mathfrak{p}$ is prime.

Proposition 3.15. Let R be a commutative ring with unity, and $\mathfrak{p}$ be a proper ideal of R. If $\mathfrak{p}$ is maximal, then $\mathfrak{p}$ is prime.

Proof. We may divide our proof into three steps.
Step 1: We prove that $\mathfrak{p}$ is maximal iff $R/\mathfrak{p}$ is a field.

$$\begin{aligned}
\mathfrak{p} \text{ is maximal} &\iff \mathfrak{p} \neq R \text{ and } \forall a \in \mathfrak{p}^c, \langle a \rangle + \mathfrak{p} = R \\
&\iff R/\mathfrak{p} \neq \{\mathfrak{p}\} \text{ and } \forall a + \mathfrak{p} \neq \mathfrak{p}, \exists x + \mathfrak{p} \in R/\mathfrak{p}, (a+\mathfrak{p})(x+\mathfrak{p}) = 1 + \mathfrak{p} \\
&\iff R/\mathfrak{p} \text{ is a field}
\end{aligned}$$

Step 2: We prove that $\mathfrak{p}$ is prime iff $R/\mathfrak{p}$ is an integral domain.

$$\begin{aligned}
\mathfrak{p} \text{ is prime} &\iff \mathfrak{p} \neq R \text{ and } \forall a, b \in \mathfrak{p}^c, ab \in \mathfrak{p}^c \\
&\iff R/\mathfrak{p} \neq \{\mathfrak{p}\} \text{ and } \forall a + \mathfrak{p}, b + \mathfrak{p} \neq \mathfrak{p}, (a+\mathfrak{p})(b+\mathfrak{p}) \neq \mathfrak{p} \\
&\iff R/\mathfrak{p} \text{ is an integral domain}
\end{aligned}$$

Step 3: As every field is an integral domain, every maximal ideal is a prime ideal.
Quod. Erat. Demonstrandum. ☐

Definition 3.16. (**Prime Element**)
Let R be a commutative ring with unity, and p be a nonunit element of R.
If $p \neq 0$ and $\forall p \nmid a, p \nmid b, p \nmid ab$, then p is prime.

Example 3.17. Let R be a commutative ring with unity. As $p \nmid a$ iff $\langle p \rangle \not\ni a$, a nonzero principal ideal $\mathfrak{p}$ is prime iff it is generated by a prime element p.

Definition 3.18. (**Irreducible Element**)
Let R be a commutative ring with unity, and p be a nonunit element of R.
If $p \neq 0$ and $\forall a, b \in (R^\times)^c, p \neq ab$, then p is irreducible.

Proposition 3.19. Let R be an integral domain, and p be a nonunit element of R. If p is prime, then p is irreducible.

Proof. Assume that p is prime.
(1) p is nonunit and nonzero.
(2) For all elements a, b of R:

$$\begin{aligned} p = ab &\implies p|ab \\ &\implies p|a \text{ or } p|b \\ &\implies 1 = (a/p)b \text{ or } 1 = a(b/p) \\ &\implies a \text{ or } b \text{ is a unit} \end{aligned}$$

Hence, p is irreducible. Quod. Erat. Demonstrandum. $\square$

Proposition 3.20. Let R be a principal ideal ring, and p be an element of R. If p is irreducible, then $\mathfrak{p} = \langle p \rangle$ is maximal.

Proof. Assume that p is irreducible.
(1) p is nonunit implies $\mathfrak{p} = \langle p \rangle$ is proper.
(2) For all ideal $\mathfrak{a} = \langle a \rangle$ of the principal ideal ring R:

$$\begin{aligned} \mathfrak{p} = \langle p \rangle \subseteq \mathfrak{a} = \langle a \rangle &\implies \exists x \in R, p = xa \\ &\implies x \text{ or } a \text{ is a unit} \\ &\implies \mathfrak{a} = \mathfrak{p} \text{ or } \mathfrak{a} = R \end{aligned}$$

Hence, $\mathfrak{p} = \langle p \rangle$ is maximal. Quod. Erat. Demonstrandum. $\square$

Remark: *Now we have the following results:*
(1) In a commutative ring with unity, $\mathfrak{p} = \langle p \rangle$ is maximal implies $\mathfrak{p} = \langle p \rangle$ is prime.
(2) In a commutative ring with unity, $\mathfrak{p} = \langle p \rangle$ is nonzero and prime iff p is prime.

(3) In an integral domain, p is prime implies p is irreducible.
(4) In a principal ideal ring, p is irreducible implies $\mathfrak{p} = \langle p \rangle$ is maximal.
If we define principal ideal domain as the conjunction of principal ideal ring and integral domain, then the four lines are equivalent.

Example 3.21. As $F[t]$ is a principal ideal domain, the followings are equivalent:
(1) An ideal $\mathfrak{p}$ is nonzero and maximal in $F[t]$.
(2) An ideal $\mathfrak{p}$ is nonzero and prime in $F[t]$.
(3) An ideal $\mathfrak{p}$ is generated by a prime polynomial $f(t) \in F[t]$.
(4) An ideal $\mathfrak{p}$ is generated by an irreducible polynomial $f(t) \in F[t]$.

Remark: *Hence, we would like to test the irreducibility of $f(t) \in F[t]$.*

Definition 3.22. (**Root**)
Let F be a field, τ be an element of F, and $f(t)$ be a polynomial in $F[t]$.
If the evaluation ring homomorphism σ_τ maps $f(t)$ to 0, then τ is a root of $f(t)$.

Proposition 3.23. Let F be a field, τ be an element of F, and $f(t)$ be a polynomial in $F[t]$. τ is a root of $f(t)$ iff $t - \tau | f(t)$.

Proof. As $t - \tau \neq 0$, we apply division algorithm to find a unique quotient polynomial $q(t) \in F[t]$ and a unique constant remainder $r \in F$, such that:

$$f(t) = q(t)(t - \tau) + r$$

As σ_τ is a ring homomorphism, we have:

$$\tau \text{ is a root of } f(t) \iff f(\tau) = \sigma_\tau(f(t)) = \sigma_\tau(r) = r = 0 \iff r = 0 \iff t - \tau | f(t)$$

Quod. Erat. Demonstrandum. $\square$

Remark: *As a corollary, if $\mathrm{Deg}(f(t)) \geq 2$ and $f(t)$ is irreducible, then $f(t)$ has no root. However, the reversed implication is true only when $n = 2$ or $n = 3$.*

Definition 3.24. (**Algebraic Multiplicity**)
Let F be a field, τ be an element of F, and $f(t)$ be a polynomial in $F[t]$.
Define the algebraic multiplicity $\mathrm{AM}_f(\tau)$ of τ as $\mathrm{Max}\{\alpha \geq 0 : (t - \tau)^\alpha | f(t)\}$.

Proposition 3.25. Let F be a field, and $f(t)$ be a nonzero polynomial in $F[t]$.

$$\sum_{\tau \in F} \mathrm{AM}_f(\tau) \leq \mathrm{Deg}(f(t))$$

Proof. We prove this statement by mathematical induction.
(1) When $\text{Deg}(f(t)) = 0$, $f(t)$ is a nonzero constant, $f(t)$ has no root, so:

$$\sum_{\tau \in F} \text{AM}_f(\tau) = 0$$

(2) For all $n \geq 0$, when $\text{Deg}(f(t)) = n$, assume the statement.
(3) When $\text{Deg}(f(t)) = n + 1$, we wish to prove the statement by inductive hypothesis.
Case 1: If $f(t)$ has no root, then:

$$\sum_{\tau \in F} \text{AM}_f(\tau) = 0 \leq n + 1$$

Case 2: If $f(t)$ has a root ω, then $\exists! q(t) \in F[t], f(t) = (t - \omega)q(t)$ and $\text{Deg}(q(t)) = n$:

$$\begin{aligned}
\sum_{\tau \in F} \text{AM}_f(\tau) &= \sum_{\tau \neq \omega} \text{AM}_f(\tau) + \text{AM}_f(\omega) \\
&= \sum_{\tau \neq \omega} \text{AM}_q(\tau) + \text{AM}_q(\omega) + 1 \\
&= \sum_{\tau \in F} \text{AM}_q(\tau) + 1 \leq n + 1
\end{aligned}$$

Hence, we've proven the statement. Quod. Erat. Demonstrandum. $\square$

Theorem 3.26. (**Fundamental Theorem of Algebra**)
Let $a(t)$ be a polynomial in $\mathbb{C}[t]$. If $\text{Deg}(a(t)) \geq 1$, then $a(t)$ has a root $\tau \in \mathbb{C}$.

Proof. Assume to the contrary that $a(t)$ has no root. WLOG, assume that:

$$a(t) = t^n + a_{n-1}t^{n-1} + \cdots, \text{where } n \geq 1$$

Define the following function from $\mathbb{S} \times [0, +\infty]$ to $\mathbb{S}$ by:

$$H(z, s) = \begin{cases} a(sz)/|a(sz)| & \text{if} \quad 0 \leq s < +\infty; \\ z^n/|z^n| & \text{if} \quad s = +\infty; \end{cases}$$

As $a(t)$ has no root, $\forall (z, s) \in \mathbb{S} \times [0, +\infty), |f(st)| \neq 0$, so $H(z, s)$ is well-defined.
The following limit suggests that $H(z, s)$ is continuous:

$$\begin{aligned}
\lim_{(z,s) \to (z_0, +\infty)} \frac{a(sz)}{|a(sz)|} &= \lim_{(z,s) \to (z_0, +\infty)} \frac{s^n z^n + a_{n-1}s^{n-1}z^{n-1} + \cdots}{|s^n z^n + a_{n-1}s^{n-1}z^{n-1} + \cdots|} \\
&= \lim_{(z,s) \to (z_0, +\infty)} \frac{z^n + a_{n-1}s^{-1}z^{n-1} + \cdots}{|z^n + a_{n-1}s^{-1}z^{n-1} + \cdots|} = \frac{z^n}{|z^n|}
\end{aligned}$$

This implies $H(z, s)$ is an inverted deformation retraction from $\{1\}$ to $\mathbb{S}$,
contradicting to $\pi_1(\{1\}) \cong \{e\} \ncong \pi_1(\mathbb{S}) \cong \mathbb{Z}$. Quod. Erat. Demonstrandum. $\square$

Definition 3.27. (**Primitive Formal Power Series**)
Let $f(t)$ be a formal power series in $\mathbb{Z}[\![t]\!]$.
If the coefficients of $f(t)$ are coprime, then $f(t)$ is primitive.

Lemma 3.28. (**Gauss's Lemma**)
Let $a(t), b(t)$ be two formal power series in $\mathbb{Z}[\![t]\!]$.
If $a(t), b(t)$ are primitive, then $a(t)b(t)$ is primitive.

Proof. Assume to the contrary that $a(t)b(t)$ is not primitive, then:

$$\exists \text{ prime } p \geq 2, p|a_0b_0 \text{ and } p|a_0b_1 + a_1b_0 \text{ and } p|a_0b_2 + a_1b_1 + a_2b_0 \text{ and } \cdots$$

As $a(t), b(t)$ are primitive, there exist minimal $r, s \geq 0$, such that $p \nmid a_r, b_s$.
Now we arrive at the following contradiction:

$$p \nmid a_0b_{r+s} + \cdots + a_{r-1}b_{s+1} + a_rb_s + a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0$$

Quod. Erat. Demonstrandum. □

Proposition 3.29. Let $f(t)$ be a primitive polynomial in $\mathbb{Z}[t]$.
$f(t)$ is irreducible in $\mathbb{Q}[t]$ iff $f(t)$ is irreducible in $\mathbb{Z}[t]$.

Proof. We may divide our proof into two parts.
"if" direction: Assume that $f(t)$ is irreducible in $\mathbb{Z}[t]$.
For all factorization $f(t) = p(t)q(t)$ in $\mathbb{Q}[t]$, we take out common factor and get $f(t) = cP(t)Q(t)$, where c is a rational number and $P(t), Q(t)$ are primitive in $\mathbb{Z}[t]$.
As both $f(t)$ and $P(t)Q(t)$ are primitive in $\mathbb{Z}[t]$, $c = \pm 1$. WLOG, assume that $c = 1$.
As $f(t)$ is irreducible in $\mathbb{Z}[t]$, $P(t) \in \mathbb{Z}[t]^\times$ or $Q(t) \in \mathbb{Z}[t]^\times$.
It follows that $p(t) \in \mathbb{Q}[t]^\times$ or $q(t) \in \mathbb{Q}[t]^\times$, so $f(t)$ is irreducible in $\mathbb{Q}[t]$.
"only if" direction: Assume that $f(t)$ is irreducible in $\mathbb{Q}[t]$.
As $\mathbb{Z}[t]$ is a subring of $\mathbb{Q}[t]$, $f(t)$ is irreducible in $\mathbb{Z}[t]$. Quod. Erat. Demonstrandum. □

Theorem 3.30. (**Eisenstein's Criterion**[3])
Let p be a prime number, and $a(t)$ be a polynomial in $\mathbb{Z}[t]$ with degree n.
If $p \nmid a_n, p|a_{n-1}, p|a_{n-2}, \cdots, p|a_1, p|a_0, p^2 \nmid a_0$, then $a(t)$ is irreducible in $\mathbb{Z}[t]$.

Proof. Assume to the contrary that $f(t)$ has a nontrivial factorization $b(t)c(t)$ in $\mathbb{Z}[t]$:

$$p|a_0 = b_0c_0 \implies p|b_0 \text{ or } p|c_0$$
$$p^2 \nmid a_0 = b_0c_0 \implies p \nmid b_0 \text{ or } p \nmid c_0$$

WLOG, assume that $p|b_0$ and $p \nmid c_0$ and $\mathrm{Deg}(b(t)) = r$, where $1 \le r \le n-1$, then:

$$\begin{aligned}
p|a_1 = b_0c_1 + b_1c_0 &\implies p|b_1c_0 \implies p|b_1 \\
p|a_2 = b_0c_2 + b_1c_1 + b_2c_0 &\implies p|b_2c_0 \implies p|b_2 \\
&\vdots \\
p|a_r = b_0c_r + b_1c_{r-1} + \cdots + b_{r-1}c_1 + b_rc_0 &\implies p|b_rc_0 \implies p|b_r
\end{aligned}$$

Now we arrive at a contradiction:

$$p|b_r \text{ and } b_r|a_n \implies p|a_n$$

Quod. Erat. Demonstrandum. □

Example 3.31. For all prime number p, **Theorem 3.30.** suggests that the following polynomial is irreducible in $\mathbb{Z}[t]$:

$$\frac{(1+t)^p - 1}{t} = \frac{1}{0!}t^{p-1} + \frac{p}{1!}t^{p-2} + \frac{p(p-1)}{2!}t^{p-3} + \cdots + \frac{p(p-1)\cdots 2}{(p-1)!}$$

Shift this polynomial, and we get a family of irreducible polynomials in $\mathbb{Z}[t]$:

$$\frac{t^p - 1}{t-1} = t^{p-1} + t^{p-2} + t^{p-3} + \cdots + 1$$

As a result, for all prime number p and integer q:

$$\cos\frac{2q\pi}{p} \in \mathbb{Q} \iff p|q \text{ or } p = 2 \text{ or } p = 3$$

4 Finite Field

4.1 Characteristic and Order

Proposition 4.1. If F is a finite field, then $n = \mathrm{Char}(F)$ is a prime number.

Proof. Assume to the contrary that $n = pq$ is a composite number, where $p, q \ge 2$. As there is a natural ring homomorphism from $\mathbb{Z}$ to F, the followings hold in F:

$$0 = n = pq \text{ and } p \neq 0 \text{ and } q \neq 0$$

This contradicts to F is a field. Quod. Erat. Demonstrandum. □

Remark: *As a result, a smaller field $\mathbb{Z}_p$ is embedded in the larger field F.*

Example 4.2. If F is a finite field, then F is a vector space over $\mathbb{Z}_p$.

Remark: *By taking a basis, we may further show that $|F| = p^n$.*

Proposition 4.3. If $f(t)$ is an irreducible polynomial in $\mathbb{Z}_p[t]$ with degree n, then $\mathbb{Z}_p[t]/\langle f(t)\rangle$ is a finite field with basis $1, u, u^2, \cdots, u^{n-1}$, where $u = t + \langle f(t)\rangle$.

Proof. We may divide our proof into three parts.
Part 1: $f(t)$ is irreducible in the principal ideal domain $\mathbb{Z}_p[t]$ implies $\mathbb{Z}_p[t]$ is a field.
Part 2: For all $c_0, c_1, c_2, \cdots, c_{n-1} \in \mathbb{Z}_p$:

$$\begin{aligned} c_0 + c_1u + c_2u^2 + \cdots + c_{n-1}u^{n-1} = 0 &\implies f(t)|c_0 + c_1t + c_2t^2 + \cdots + c_{n-1}t^{n-1} \\ &\implies c_0 + c_1t + c_2t^2 + \cdots + c_{n-1}t^{n-1} = 0 \\ &\implies c_0 = c_1 = c_2 = \cdots = c_{n-1} = 0 \end{aligned}$$

Part 3: For all $g(u) \in \mathbb{Z}_p[t]/\langle f(t)\rangle$, as $f(t) \neq 0$, we may apply division algorithm to find $q(t) \in \mathbb{Z}_p[t]$ and $c_0, c_1, c_2, \cdots, c_{n-1} \in \mathbb{Z}_p$, such that:

$$\begin{aligned} g(t) &= q(t)f(t) + c_0 + c_1t + c_2t^2 + \cdots + c_{n-1}t^{n-1} \\ g(u) &= q(u)f(u) + c_0 + c_1u + c_2u^2 + \cdots + c_{n-1}u^{n-1} \\ &= c_0 + c_1u + c_2u^2 + \cdots + c_{n-1}u^{n-1} \end{aligned}$$

Hence, $\mathbb{Z}_p[t]/\langle f(t)\rangle$ is a finite field with basis $1, u, u^2, \cdots, u^{n-1}$.
Quod. Erat. Demonstrandum. □

4.2 Field Extension

Example 4.4. Every quotient map $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ fails to preserve characteristic.

Proposition 4.5. Let F, F' be two fields.
Every ring homomorphism $\sigma : F \to F'$ is injective.

Proof. Assume to the contrary that $\text{Ker}(\sigma) \neq \{0\}$. As F is a field, the ideal $\text{Ker}(\sigma) = F$. This implies $0' = \sigma(1) = 1'$, contradicting to $F' \neq \{0'\}$. Quod. Erat. Demonstrandum. □

Remark: *As a result, every ring homomorphism $\sigma : F \to F'$ preserves characteristic.*

Definition 4.6. (**Field Extension**)
Let F, F' be two fields.
If there exists a ring homomorphism $\sigma : F \to F'$, then F' is an extension of F.

Example 4.7. Let F be a field, and $f(t)$ be an irreducible polynomial in $F[t]$.
$F[t]/\langle f(t)\rangle$ is an extension of F.

4.3 Primitive Root

Definition 4.8. (**Primitive Root**)
Let R be a commutative ring with unity, and g be an element of R.
If g generates the group $R^\times$ of units, then g is a primitive root of R.

Example 4.9. In $\mathbb{Z}_8$, $\mathbb{Z}_8^\times$ is isomorphic to K_4, so $\mathbb{Z}_8$ has no primitive root.

Theorem 4.10. Every finite field F has a primitive root g.

Proof. Assume to the contrary that some finite field F has order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}+1$, where $p_1, p_2, \cdots, p_m$ are distinct prime numbers, $\alpha_1, \alpha_2, \cdots, \alpha_m$ are positive integers, and the p_1-part P_1 of $F^\times$ has at least two cyclic components. Assume that:

$$\begin{gathered} P_1 \cong P_{1,1} \times P_{1,2} \times \cdots \\ |P_{1,1}| = p_1^{n_{1,1}} \text{ and } |P_{1,2}| = p_1^{n_{1,2}} \text{ and } \cdots \\ n_{1,1} \geq 1 \text{ and } n_{1,2} \geq 1 \text{ and } \cdots \end{gathered}$$

Consider the following polynomial in $F[t]$:

$$f(t) = t^{|P_{1,1}|} - 1$$

As the multiplicative order $\mathrm{Ord}(\tau)$ of all $\tau \in P_{1,1}$ divides $|P_{1,1}|$, τ is a root of $f(t)$.
As $P_{1,2}$ is a p_1-group, $P_{1,2}$ has an element ξ of order p_1, which is also a root of $f(t)$.
Now we arrive at the following contradiction:

$$\sum_{\tau \in F} \mathrm{AM}_f(\tau) > |P_{1,1}| = \mathrm{Deg}(f(t))$$

Hence, $|F|$ must be in the form $p_1p_2\cdots p_m+1$, and $F^\times$ is cyclic.
Quod. Erat. Demonstrandum. $\square$

Remark: *However, it is hard to find this primitive root, so we stop here.*

References

[1] H. Ren, “Template for math notes,” 2021.

[2] M. user, “Intersection of principal ideals is not principal,” https://mathoverflow.net/questions/443334/intersection-of-principal-ideals-is-not-principal, 2023, accessed: 2023-10-17.

[3] Wikipedia contributors, “Eisenstein’s criterion — Wikipedia, the free encyclopedia,” 2024, [Online; accessed 19-December-2024]. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Eisenstein%27s_criterion&oldid=1247464065