MAT347: Groups, Rings and Fields

QiLin Xue

Fall 2021

Contents

1 Ring Theory

1.1 Eisenstein's Criterion

Lemma 1: Eisenstein's Criterion: Of $f(x) \in \mathbb{Z}[x]$,

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

and if p is a prime such that $p|a_i$ for all $i = 0, 1, \ldots, a_{n-1}$ but p^2 does not divide a_0 then f is irreducible.

Proof. Suppose

$$f(x) = (x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0)(x^\ell + c_{\ell-1}x^{\ell-1} + \cdots + c_1 x + c_0).$$

Then take the constant term $a_0 = b_0 c_0$. One of b_0, c_0 is not divisible by p so WLOG let b_0 not divisible by p. Modulo p, we have

$$\begin{aligned} f(x) &= x^n \\ &= (x^k + \cdots + b_0)(x^\ell + \cdots + 0) \\ &= x^k + \cdots, \end{aligned}$$

where b_0 is nonzero mod p. Whichever coefficient is nonzero mod p with the highest power of x (other than x^k, x^ℓ) will give a nonzero term in the product.

NB: There is some subtlety to this last step. We should consider the term where we multiply b_n by the lowest nonzero term in the second factor. Then we can show there is no other term with the same degree that can cancel it out. □

For example, for any odd prime p,

$$f(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Now consider $f(x+1)$. Then,

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{1}{x}\left(x^p + px^{p-1} + \binom{p}{2} + \cdots + px\right) \\ &= x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p. \end{aligned}$$

Note that all the binomial coefficients are divisible by p. The constant coefficient is p, so $f(x+1)$ is an Eisenstein polynomial, and therefore it is irreducible. We can now extend Eisenstein's Criterion to be in general,

Theorem: Eisenstein's Criterion for UFD: If R is a UFD, and $f(x) \in R[x]$, is such that there is some prime ideal P such that f is monic but all its coefficients except the first are in P and the constant term is not in P^2, then f is irreducible.

Theorem: If F is a field, then the maximal ideals in $F[x]$ are of the form $(g(x))$, where $g(x)$ is irreducible.

That is, $F[x]/(g(x))$ is a field if and only if $g(x)$ is irreducible. This implies that

$$\mathbb{Q}[x]/(x^2 + 1) \tag{1.1}$$

is a field since $x^2 + 1$ has no roots in $\mathbb{Q}$. Similarly, $\mathbb{R}[x]/(x^2+1)$ is a field, and we can conclude that

$$\mathbb{R}[x]/(x^2 + 1) = (\bar{1}, \bar{x}) \cong \mathbb{C}, \tag{1.2}$$

with $\bar{x}^2 = -1$.

If $f(x) \in F[x]$, we can factor it as

$$f(x) = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \tag{1.3}$$

with $p_i(x) \in F[x]$ are irreducible. Let us assume that the p_is are distinct. By the Chinese Remainder Theorem,

$$F[x]/(f(x)) \cong F[x](p_1(x)^{a_1}) \times \cdots \times F[x]/(p_r(x)^{a_r}).$$

We'll come back to this later.

Proposition 1: If $a_1, \ldots, a_r$ are roots of $f(x)$, then $f(x) \in F[x]$ is divisible by $(x-a_1)(x-a_2)\cdots(x-a_r)$.

While quite simple, this leads to an interesting corollary,

Corollary 1: Given any field F, any finite subgroup of H of the multiplicative group $F^\times$ of F must be cyclic.

We know that, from the classification of finite abelian groups,

$$H \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_k} \tag{1.4}$$

where $m_1|m_2|\cdots|m_k$. Every element of $x \in C_{m_k}$ satisfies $x^{m_k} = 1$. But since $m_i|m_k$, we also know that $x^{m_k} = 1$ is also true for any $x \in C_{m_i}$.

If $k > 1$, there are more than m_k roots of $x^{m_k} - 1$, so we have a contradiction, and we must have $k = 1$.

Corollary, the multiplicative group of any finite field is cyclic.

1.2 Noetherian Rings

Definition: A ring R is Noetherian if every ideal I is R if finitely generated.

As a non-example, $F[x_1, x_2, \ldots]$ with an infinite number of variables is not Noetherian as $I = (x_1, x_2, \ldots)$ is the ideal of polynomials with constant coefficients is not finitely generated.

Theorem: Hilbert's Basis Theorem: If R is Noetherian, then $R[x]$ is Noetherian.

2 Modules

Definition: Suppose R is a ring. A module M is an abelian group $(M, +)$ equipped with an action of R

$$R \times M \to M, \qquad (r, m) \mapsto rm, \tag{2.1}$$

such that
(i) $(r+s)m = rm + sm$
(ii) $r(m+n) = rm + rn$
(iii) $(rs)m = r(sm)$
(iv) If R has identity, then $1m = m$.
Note that if R has no identity, $rm = 0$ for all r, m is a possibility.

To be specific, the above is a left module, but the same thing can be applied to a right module. If M is an R-module, a submodule is a subgroup $N \leq M$ (relative to $+$) such that $rn \in N \forall r \in R, n \in N$.

Some examples,

- If R is a ring, then it is a module over itself. Submodules are then ideals.
- If $R = F$ is a field, then any F-module V is a vector space over F. However, we should not expect modules to be like vector spaces in general. If we write $R^n = (r_1, \ldots, r_n) = R \times \cdots R$ with componentwise addition and multiplication, R^n is an R-module, called the **free R-module of rank n.**
- Suppose that $R = \mathbb{Z}$. Then any $\mathbb{Z}$-module M is an abelian group, and vice versa (i.e. the conditions don't add any extra structure)

- Suppose F is a field, V is a vector space over F and $T : V \to V$ is an F-linear operator. Then V becomes a $F[x]$-module by letting
$$xv = Tv, \qquad (a_n x^n + \cdots a_1 x + a_0)v = a_n T^n v + \cdots + a_1 Tv + a_0 v \tag{2.2}$$
Note that $F[x]$ has many module structures on V, one for each T. What is an $F[x]$-submodule of V?
  - A **T-stable** subspace W (i.e. $T(W) \leq W$) is also called a subspace preserved by T.
- Suppose F is a field, G is a group, and recall the group ring
$$F[G] = \left\{ \sum_{i=1}^{n} a_i g_i | a_i \in F, g_i \in G \right\}, \tag{2.3}$$
if there is an action of G on an F-vector space V then V becomes a $F[G]$-module.

  Suppose M is an R-module. Suppose $I \subset R$ is an ideal such that $i \cdot m = 0 \forall i \in I, \forall m \in M$. Then we say I **annhilates** M. In this case, the obvious choice of R/I on M is well-define: $(r+I)m = rm$ and $(r+i+I)m = (r+i)m = rm+0 = rm$.

Definition: Supopse R is commutative ring with identity 1_R. Suppose A is a ring with identity 1_A and suppose there exists a homomorphism
$$\varphi : R \to A$$
such that $\varphi(1_R) = 1_A$ and $\varphi(R) \subseteq Z(A)$, then A is called an R-algbra.

For example,

- let $R = F$ be a field and $A = F[x]$, and $\varphi(r) = r$ (a constant polynomial).
- This also works for any commutative ring R with 1 and $A = R[x]$ and it also works for commutative rings $R \subset S$ with $1_R = 1_S$. For example, $S[x]$ is an R-algebra and $\mathbb{C}[x]$ is an $\mathbb{Q} - algebra$ and a $\mathbb{Z} - algebra$.
- Also true for group rings! If R is commutative with identity, then $R[G]$ is an R-algebra for any (finite) group G. Note, the algebra may no longer be commutative.
- Perhaps the most important example, let $R = F$ be a field and $A = M_{n \times n}(F)$. Let $\varphi(r) = r \cdot \text{id}_n$.
- One non-trivial example: $\mathbb{F}_p[x]$ is a $\mathbb{Z}$-algebra, where $\varphi(n) = n + p\mathbb{Z} \in \mathbb{F}_p$.

Definition: If A is an R-module then $B \subseteq A$ is an R-submodule if it is closed under addition and multiplication.

Proposition 2: If R contains 1, then it is sufficient to check $(b + rc) \in B$ for all $b, c \in B, r \in R$.

Definition: If A, B are R-modules, then $\varphi : A \to B$ is an R-homomorphism if $\varphi(a+b) = \varphi(a)+\varphi(b)$ and $\varphi(rm) = r\varphi(m)$ for all $a, b \in A$ and $r \in R$.

In this case, $|\varphi\rangle$ is an R-submodule of A and $\varphi(A)$ is an R-submodule of B.

You can always take the quotient between a module and a submodule. That is, if $A \subseteq B$ are R-modules, then B/A is an R-submodule.

An example from linear algebra is that
$$T(V) \cong V/\ker(T). \tag{2.4}$$

Definition: We write $HOM_R(M, N)$ for the set of R-module homomorphisms $f : M \to N$ (where M, N are R-modules).

Notice: $\text{HOM}_R(M, N)$ is an R-module. If $f, g \in \text{HOM}_R(M, N)$, $r \in R$, then $(f+g)(m) = f(m)+g(m)$ and $(rf)(m) = rf(m)$.

If $f \in \text{HOM}_R(M, N)$ and $g \in \text{HOM}_R(N, P)$ then $g \circ f \in \text{HOM}_R(M, P)$. Therefore, $\text{HOM}_R(M, M)$ is a ring. This ring is called the **endomorphism ring** of M. It is interchangeably called $\text{END}_R(M)$.

TESTABLE MATERIAL ENDS (END OF 10.2)

Assume that R has an identity. If M is an R-module and $A \subset M$ is a (possibly finite) subset, then there is a **free module on A,** the set of all finite R-combinations of elements of A,

$$\{\sum_{i=1}^{n} r_i a_i | r_i \in R, a_i \in A\}.$$

This is a set of formal sums, *not* a subset of A.

Definition: If $N_1, \ldots, N_n \subseteq M$ are R-submodules of M, their sum is

$$N_1 + \cdots + N_n = \left\{ \sum_{i=1}^{n} r_i n_i | r_i \in R, n_i \in N_i \right\} \tag{2.5}$$

It is easy to show that this is an R-submodule of M, the smallest one that contains all the N_is.

Definition: If $A \subseteq M$, and A is a subset of R-module M, then

$$RA = \left\{ \sum_{i=1}^{n} r_i a_i | r_i \in R, a_i \in A \right\}. \tag{2.6}$$

RA is an R-submodule of M, the smallest such that contains A. Even if A is infinite, we still only have finite sums.

If $N_1, \ldots, N_n$ are R-modules, consider the product

$$N_1 \times N_2 \times \cdots \times N_n = \{(n_1, n_2, \ldots, n_n) | n_i \in N_i\}. \tag{2.7}$$

If each N_i is a submodule of M then there is a map $\varphi : N_1 \times N_2 \times \cdots \times N_n \to M$ defined by $(n_1, n_2, \ldots, n_n) \mapsto n_1 + \cdots + n_n$.

If φ is an isomorphism, $\ker \varphi = \{0\}$. Note: missing some stuff here onwards.

Remarks: If $R = F$ is a field, then R-direct sums are just vector space direct products, i.e.

$$N_1 \oplus \cdots \oplus N_n \cong N_1 \times \cdots \times N_n. \tag{2.8}$$

This remark is worth making because it is not true for infinite products and sums.

Example 1: In $F[X]$, let $A = \{1, x\}$, then

$$FA = \{a + bx | a, b \in F\}. \tag{2.9}$$

But note that A generates $F[x]$ as a ring, even though it does not generate it as an F-module.

If M is an R-module and $A \subseteq M$ such that $M = RA$ then we say A generates M. If $M = RA$ for some finite set A, then M is finitely generated.