Algebra III Revision Notes

Kexing Ying

May 17, 2022

Ring Theory

In a PID

$$\text{prime} \iff \text{irreducible} \iff \text{maximal ideal} \iff \text{quotient is a field} \iff \text{quotient ID}.$$

To find irreducible elements in a Euclidean domain, note that

- invertible elements have norm 1
- elements have prime norm iff irreducible (Gaussian integers $a + bi$, $ab \neq 0$)

Finding GCD in (multiplicative) Euclidean domain:

- compute the norms
- find GCD of the norms l, the norm of the GCD must divide l
- find the elements which has norm dividing l

Given ideals $I = \langle a_i \mid i \in \mathcal{I} \rangle, J = \langle b_j \mid j \in \mathcal{J} \rangle$,

$$IJ = \langle a_i b_j \mid i \in \mathcal{I}, j \in \mathcal{J} \rangle.$$

In a Euclidean domain (requires $N(ab) = N(a)N(b) \geq N(a)$) R, $N(a) = N(1)$ iff $a \in R^\times$.

Show ideal not principle in $\mathbb{Z}[\sqrt{-n}]$: Define the multiplicative function $N : \mathbb{Z}[\sqrt{-n}] \to \mathbb{N} : a+b\sqrt{-n} \mapsto a^2+nb^2$. Then, if $\langle \alpha, \beta \rangle = \langle \gamma \rangle$, $N(\gamma) \mid N(\alpha), N(\beta)$, from this show contradiction.

Field Extensions

We will in this section denote $K \subseteq L$ fields and assume L as a vector space over K has finite dimension.

Definition (Degree)**.** Let $K \subseteq L$ be fields. Then $[L : K] := \dim_K L$ is the degree of L over K.

Theorem. Given field extensions $K \subseteq L \subseteq M$,

$$[M : L][L : K] = [M : K].$$

Given $\alpha \in L$ we define the evaluation map $\text{ev}_\alpha : K[X] \to L : P(X) \mapsto P(\alpha)$. We have the following observations.

- assume $\ker \text{ev}_\alpha \neq \{0\}$ and so, as $K[X]$ is a PID (as it is an Euclidean domain), there exists some $P(X) \in K[X]$ such that $\ker \text{ev}_\alpha = \langle P(X) \rangle$. We call $P(X)$ is *minimal polynomial* of α;
- as $\text{Im}(\text{ev}_\alpha)$ is a subring of K, $K[X]/\langle P(X) \rangle \simeq \text{Im}(\text{ev}_\alpha)$ is an integral domain, and so, $\langle P(X) \rangle$ is a prime ideal;
- recalling that non-zero prime ideals in a PID are maximal, $K[X]/\langle P(X) \rangle$ is in fact a field;
- we denote $K(\alpha)$ as $K[X]/\langle P(X) \rangle$.

Theorem. Applying quotient remainder using the Euclidean norm on $K[X]$, $[K(\alpha) : K] = \deg P(X)$.

Theorem. If $[L : K] < \infty$, then every element of L is algebraic over K, i.e. for all $\alpha \in L$, there exists $P(X) \in K[X]$ such that $P(\alpha) = 0$. This follows as $1, \alpha, \cdots, \alpha^{[L:K]}$ is linear dependent as vectors in L over K.

Theorem. If K has characteristics p, then the map $x \mapsto x^q$ is a field endomorphism and is known as the Frobenious endomorphism.

Theorem. If $|K| = q = p^r$, then the map $x \mapsto x^q$ is a field automorphism.

Theorem. If A is an abelian group such that $|A| = n$ and for all $d \mid n$, A has exactly d elements of order dividing d, then A is cyclic.

Corollary. $K^\times$ is cyclic since $X^{p^r-1} - 1$ factors into $p^r - 1$ distinct roots in K and has divisor $X^d - 1$ for every $d \mid |K|$.

Theorem. If K has characteristics p, then $K = \mathbb{F}_p(\alpha)$ for some α. Namely, we consider K as a field extension of $\mathbb{F}_p$ by recalling the theory of prime fields.

Theorem. All irreducible polynomials of $K[X]$ where $|K| = q = p^s$ of degree r appears exactly once in the divisors of $X^{q^r} - X$.

Corollary. Any two finite fields of the same cardinality are isomorphic.

Over $\mathbb{F}_p$, $P(X^p) = P(X)^p$ as $X \mapsto X^p$ is a field automorphism.

Product of roots of a monic polynomial is the $(-1)^d c_0$ where c_0 is the constant coefficient. So, if the $c_0 = 1$ of a monic polynomial in $\mathbb{Z}[X]$, the roots must be ± 1 which can be manually checked.

One may apply the quadratic formula for a degree 2 polynomial in $\mathbb{C}[X, Y]$.

Given $P(X), Q(X) \in K[X]$, P irreducible. Then, if P, Q share a root $P \mid Q$ (proof by considering their GCD cannot be 1 by Bezout).

Use **derivatives** to show polynomial has no repeated factors (show it has no shared roots with its derivative).

Product of roots = constant coeff. of monic (useful for checking the degree 3 polynomial is irreducible).

Factorisation in UFD

Theorem (Gauss's Lemma)**.** Let R be a UFD and let $P(X), Q(X) \in R[X]$ be primitive (i.e. coefficients have GCD 1), then the produce $P(X)Q(X)$ is also primitive.

Corollary. If $P(X) \in R[X]$ has a divisor $A(X) \in K[X]$ where K is the field of fraction of R, then there exists some $\alpha \in K^\times$ such that $\alpha A(X) \in R[X]$ and $\alpha A(X) \mid P(X)$.

Corollary. If R is a UFD then so is $R[X]$.

Proposition. Let $P(X) \in R[X]$. $P(X)$ is irreducible if and only if $Q_r(X) := r^d P(X/r)$ is irreducible for any $r \in R$ where $d = \deg P(X)$.

Proposition. Let $P(X) \in R[X]$ be monic and let I be a prime ideal of R. Then, if $P(X)$ is irreducible as a polynomial in $R/I[X]$, then $P(X)$ is irreducible in $R[X]$.

Proposition (Eisenstein's Criterion)**.** Let $P(X) = c_0 + c_1 X + \cdots + X^n$ be a monic polynomial in $R[X]$ and let I be a prime ideal of R. Then, if for all $0 \leq i \leq n-1$, $c_i \in I$ and $c_0 \notin I^2$, then $P(X)$ is irreducible in $R[X]$.

Showing $\sum_{i=0}^n X^i$ is irreducible in $\mathbb{Q}[X]$: write $T = X - 1$ and we observe

$$\sum_{i=0}^{n} X^i = \frac{X^{n+1}-1}{X-1} = \frac{(T+1)^{n+1}-1}{T} = T^n + \cdots =: P(T)$$

where by the binomial formula, all non-leading coefficients of $P(T)$ are divisible by $n+1$ while the constant term is $n+1$ and so not divisible by $(n+1)^2$. Thus, if $n+1$ is prime, we may conclude irreducibility by Eisentein's. Alternative adjustments can be made if $n+1$ is not prime.

Module Theory

Basic concepts: module, submodule, generating set, finitely generated, quotient, direct sum, module homomorphism, kernel, image, universal property for modules, free module, universal property of free modules.

Let M be any R-module with generating set S. Then, by the universal property of free modules, we have the natural homomorphism $\tilde{\iota} : R[S] \to M$ induced by the inclusion map $\iota : S \hookrightarrow M$. Now, denoting $K = \ker \tilde{\iota}$, let T be a generating set of K, we have the short exact sequence

$$0 \to R[T] \to R[S] \to M \to 0.$$

Hence, denoting the first map by ϕ, we have the isomorphism

$$M \simeq R[S]/\phi(R[T])$$

and this is called a presentation of M. If both modules in the quotient have finite rank, M is called finitely presented. In the case both $|S| = n, |T| = m$ are finite, one can encode the information of M into a presentation matrix Φ where

$$\phi(t_i) = \sum_{j=1}^{n} \Phi_{ji} s_j.$$

Namely, $\Phi : R^m \to R^n$ is a homomorphism such that

$$M \simeq R^n/\Phi R^m.$$

Elementary column operations changes the relation to an equivalent set of relations while elementary row operations changes the generating set.

Smith normal form algorithm on the matrix A over a Euclidean domain:

The main step is to write A in a form such that a_{11} is the only non-zero entry in the first row and the first column such that a_{11} divides every entry of A.

- Exchange rows and column such that a_{11} has the smallest Euclidean norm.
- Applying Euclidean algorithm to make each entry of the first row and column have norm strictly less than a_{11} by adding multiples of the first row and column to the other rows and columns.
- Repeat the above two steps until all entries of the first row and column are zero.
- Now, if there is some a_{ij} not divisible by a_11, add the i-th column to the first (this does not change a_{11} as $a_{1i} = 0$).
- Repeat from step 1 (this will decrease the norm of a_{11}).

Then, applying this algorithm to the minors of A inductively, we end up with the Smith normal form of A.

Theorem (Classification of finitely generated modules over a Euclidean domain)**.** Let M be a finitely generated module over a Euclidean domain R. Then, there exists a unique integer r and non-units $a_1, \cdots, a_n$ of R such that $a_i \mid a_{i+1}$ and

$$M \simeq R^r \oplus R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle \oplus \cdots \oplus R/\langle a_n \rangle.$$

The above classification holds for PID as well though we did not prove it.

Corollary. Let A be a finitely generated abelian group. Then there is a unique integer r and integers $a_1, \cdots, a_t > 1$ with $a_1 \mid a_2 \mid \cdots \mid a_t$ such that

$$A \simeq \mathbb{Z}^r \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_t\mathbb{Z}.$$

Let K be a field, V a finite dimensional K-vector space and let $L : V \to V$ a linear map, then we define the $K[T]$-module (or $K[X]$-module) M_L by taking the underlying set V and defining scalar multiplication by

$$P(T) \cdot v := P(L)(v)$$

for all $P(T) \in K[T]$ and $v \in V$ where $P(L) : V \to V$ is the linear map obtained by applying P on L.

It is clear that a basis $\{v_1, \cdots, v_m\}$ of V generates M_L as a $K[T]$-module. Furthermore, writing A the matrix corresponding to L with respect to this basis so that $Lv_i = \sum_{j=1}^m a_{ji} v_j$, we have the relations $T \in K[T]$, $T \cdot v_i = Lv_i = \sum_{j=1}^m a_{ji} v_j$. These relations generate all relations. Thus, M_L has presentation matrix $T\mathrm{id}_m - A$.

Now, as M_L is finitely generated as a $K[T]$-module, by the classification of finitely generated modules, we have $P_1(T), \cdots, P_t(T) \in K[T]$ such that $P_1(T) \mid \cdots \mid P_t(T)$ and

$$M_L \simeq K[T]/\langle P_1(T)\rangle \oplus \cdots \oplus K[T]/\langle P_t(T)\rangle.$$

where the rank is 0 as the number of generators of M_L equals the number of generators of the relations.

Now, by considering $K[T]/\langle P(T)\rangle$ has basis $1, T, \cdots, T^{d-1}$ where $d = \deg P(T)$, L restricted on $K[T]/\langle P(T)\rangle$ has action "multiplication by T" represented by the companion matrix of $P(T)$ with respect to this basis. Hence, we have the rational canonical form of L given by block matrices for which the i-th block is the companion matrix of $P_i(T)$.

Thus, if K is algebraically closed, each $P_i(T)$ can be factored into a product of linear factors which allows us to conclude the Jordan normal form theorem.

Writting

$$M_L \simeq K[T]/\langle P_1(T)\rangle \oplus \cdots \oplus K[T]/\langle P_t(T)\rangle,$$

the minimal polynomial of L is P_t and the characteristic polynomial of L is $\prod P_i$.

The minimal polynomial of a linear map L is the unique monic generator of the ideal $\{P(T) \mid P(L) = 0\}$ of $K[T]$.

Noetherian

Definition (Notherian)**.** An R-module M is Noetherian if every increasing chain of M-submodules stabilizes.

Theorem. An R-module M is Noetherian if and only if every M-submodule is finitely generated.

Corollary. Any PID is Noetherian over itself.

Some properties of Noetherian modules:

- The quotient of Noetherian modules is Noetherian.
- If $N \leq M$ is Noetherian and M/N is Noetherian, then so is M.
- Direct sums of Noetherian modules is Noetherian.
- R Noetherian implies R^k Noetherian as it is a direct sum of k-copies of R.
- If R is a Noetherian ring and $f : R \to S$ is a surjective ring homomorphism, then S is Noetherian.

Theorem. Any finitely generated module over a Noetherian ring is Noetherian.

Theorem (Hilbert Basis Theorem)**.** R is Noetherian if and only if $R[X]$ is Noetherian.