Part IB — Groups, Rings and Modules
Theorems

Based on lectures by O. Randal-Williams
Notes taken by Dexter Chua

Lent 2016

Groups
Basic concepts of group theory recalled from Part IA Groups. Normal subgroups, quotient groups and isomorphism theorems. Permutation groups. Groups acting on sets, permutation representations. Conjugacy classes, centralizers and normalizers. The centre of a group. Elementary properties of finite p-groups. Examples of finite linear groups and groups arising from geometry. Simplicity of A_n.

Sylow subgroups and Sylow theorems. Applications, groups of small order. [8]

Rings
Definition and examples of rings (commutative, with 1). Ideals, homomorphisms, quotient rings, isomorphism theorems. Prime and maximal ideals. Fields. The characteristic of a field. Field of fractions of an integral domain.

Factorization in rings; units, primes and irreducibles. Unique factorization in principal ideal domains, and in polynomial rings. Gauss' Lemma and Eisenstein's irreducibility criterion.

Rings $\mathbb{Z}[\alpha]$ of algebraic integers as subsets of $\mathbb{C}$ and quotients of $\mathbb{Z}[x]$. Examples of Euclidean domains and uniqueness and non-uniqueness of factorization. Factorization in the ring of Gaussian integers; representation of integers as sums of two squares.

Ideals in polynomial rings. Hilbert basis theorem. [10]

Modules
Definitions, examples of vector spaces, abelian groups and vector spaces with an endomorphism. Sub-modules, homomorphisms, quotient modules and direct sums. Equivalence of matrices, canonical form. Structure of finitely generated modules over Euclidean domains, applications to abelian groups and Jordan normal form. [6]

Contents

0 Introduction

1 Groups

1.1 Basic concepts

Lemma. The inverse of an element is unique.

Lemma. $H \subseteq G$ is a subgroup if H is non-empty and for any $h_1, h_2 \in H$, we have $h_1 h_2^{-1} \in H$.

Theorem (Lagrange's theorem)**.** Let G be a finite group, and $H \leq G$. Then

$$|G| = |H||G : H|,$$

where $|G : H|$ is the number of H-cosets in G.

Lemma. If G is a finite group and $g \in G$ has order n, then $n \mid |G|$.

1.2 Normal subgroups, quotients, homomorphisms, isomorphisms

Lemma. If $\phi : G \to H$ is a homomorphism, then

$$\phi(g^{-1}) = \phi(g)^{-1}.$$

Lemma. For a homomorphism $\phi : G \to H$, the kernel $\ker(\phi)$ is a *normal subgroup*, and the image $\mathrm{im}(\phi)$ is a subgroup of H.

Lemma. If ϕ is an isomorphism, then the inverse ϕ^{-1} is also an isomorphism.

Theorem (First isomorphism theorem)**.** Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi) \lhd G$ and

$$\frac{G}{\ker(\phi)} \cong \mathrm{im}(\phi).$$

Theorem (Second isomorphism theorem)**.** Let $H \leq G$ and $K \lhd G$. Then $HK = \{h \cdot k : h \in H, k \in K\}$ is a subgroup of G, and $H \cap K \lhd H$. Moreover,

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Theorem (Third isomorphism theorem)**.** Let $K \leq L \leq G$ be normal subgroups of G. Then

$$\frac{G}{K} \Big/ \frac{L}{K} \cong \frac{G}{L}.$$

Lemma. An abelian group is simple if and only if it is isomorphic to the cyclic group C_p for some prime number p.

Theorem. Let G be any finite group. Then there are subgroups

$$G = H_1 \rhd H_2 \rhd H_3 \rhd H_4 \rhd \cdots \rhd H_n = \{e\}.$$

such that H_i/H_{i+1} is simple.

1.3 Actions of permutations

Lemma. An action of G on X is equivalent to a homomorphism $\phi : G \to \mathrm{Sym}(X)$.

Proposition. $G_X \lhd G$ and $G/G_X \cong G^X$.

Theorem. Let G be a finite group, and $H \leq G$ a subgroup of index n. Then there is a normal subgroup $K \lhd G$ with $K \leq H$ such that G/K is isomorphic to a subgroup of S_n. Hence $|G/K| \mid n!$ and $|G/K| \geq n$.

Corollary. Let G be a non-abelian simple group. Let $H \leq G$ be a proper subgroup of index n. Then G is isomorphic to a subgroup of A_n. Moreover, we must have $n \geq 5$, i.e. G cannot have a subgroup of index less than 5.

Theorem (Orbit-stabilizer theorem)**.** Let G act on X. Then for any $x \in X$, there is a bijection between $G \cdot x$ and G/G_x, given by $g \cdot x \leftrightarrow g \cdot G_x$.

In particular, if G is finite, it follows that

$$|G| = |G_x||G \cdot x|.$$

1.4 Conjugacy, centralizers and normalizers

Proposition. Let G be a finite group. Then

$$|\operatorname{ccl}(x)| = |G : C_G(x)| = |G|/|C_G(x)|.$$

Theorem. The alternating groups A_n are simple for $n \geq 5$ (also for $n = 1, 2, 3$).

1.5 Finite p-groups

Theorem. If G is a finite p-group, then $Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}$ is non-trivial.

Lemma. For any group G, if $G/Z(G)$ is cyclic, then G is abelian.

In other words, if $G/Z(G)$ is cyclic, then it is in fact trivial, since the center of an abelian group is the abelian group itself.

Corollary. If p is prime and $|G| = p^2$, then G is abelian.

Theorem. Let G be a group of order p^a, where p is a prime number. Then it has a subgroup of order p^b for any $0 \leq b \leq a$.

1.6 Finite abelian groups

Theorem (Classification of finite abelian groups)**.** Let G be a finite abelian group. Then there exist some $d_1, \cdots, d_r$ such that

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r}.$$

Moreover, we can pick d_i such that $d_{i+1} \mid d_i$ for each i, and this expression is unique.

Lemma. If n and m are coprime, then $C_{mn} \cong C_m \times C_n$.

Corollary. For any finite abelian group G, we have

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r},$$

where each d_i is some prime power.

1.7 Sylow theorems

Theorem (Sylow theorems)**.** Let G be a finite group of order $p^a \cdot m$, with p a prime and $p \nmid m$. Then

(i) The set of Sylow p-subgroups of G, given by

$$\mathrm{Syl}_p(G) = \{P \leq G : |P| = p^a\},$$

is non-empty. In other words, G has a subgroup of of order p^a.

(ii) All elements of $\mathrm{Syl}_p(G)$ are conjugate in G.

(iii) The number of Sylow p-subgroups $n_p = |\mathrm{Syl}_p(G)|$ satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid |G|$ (in fact $n_p \mid m$, since p is not a factor of n_p).

Lemma. If $n_p = 1$, then the Sylow p-subgroup is normal in G.

Corollary. Let G be a non-abelian simple group. Then $|G| \mid \frac{n_p!}{2}$ for every prime p such that $p \mid |G|$.

2 Rings

2.1 Definitions and examples

2.2 Homomorphisms, ideals, quotients and isomorphisms

Lemma. A homomorphism $\phi : R \to S$ is injective if and only if $\ker \phi = \{0_R\}$.

Lemma. If $\phi : R \to S$ is a homomorphism, then $\ker(\phi) \lhd R$.

Proposition. The quotient ring is a ring, and the function

$$\begin{aligned} R &\to R/I \\ r &\mapsto r + I \end{aligned}$$

is a ring homomorphism.

Proposition (Euclidean algorithm for polynomials)**.** Let $\mathbb{F}$ be a field and $f, g \in \mathbb{F}[X]$. Then there is some $r, q \in \mathbb{F}[X]$ such that

$$f = gq + r,$$

with $\deg r < \deg g$.

Theorem (First isomorphism theorem)**.** Let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi) \lhd R$, and

$$\frac{R}{\ker(\phi)} \cong \mathrm{im}(\phi) \leq S.$$

Theorem (Second isomorphism theorem)**.** Let $R \leq S$ and $J \lhd S$. Then $J \cap R \lhd R$, and

$$\frac{R + J}{J} = \{r + J : r \in R\} \leq \frac{S}{J}$$

is a subring, and

$$\frac{R}{R \cap J} \cong \frac{R + J}{J}.$$

Theorem (Third isomorphism theorem)**.** Let $I \lhd R$ and $J \lhd R$, and $I \subseteq J$. Then $J/I \lhd R/I$ and

$$\left(\frac{R}{I}\right) \Big/ \left(\frac{J}{I}\right) \cong \frac{R}{J}.$$

2.3 Integral domains, field of factions, maximal and prime ideals

Lemma. Let R be a finite ring which is an integral domain. Then R is a field.

Lemma. Let R be an integral domain. Then $R[X]$ is also an integral domain.

Theorem. Every integral domain has a field of fractions.

Lemma. A (non-zero) ring R is a field if and only if its only ideals are $\{0\}$ and R.

Lemma. An ideal $I \lhd R$ is maximal if and only if R/I is a field.

Lemma. An ideal $I \lhd R$ is prime if and only if R/I is an integral domain.

Proposition. Every maximal ideal is a prime ideal.

Lemma. Let R be an integral domain. Then its characteristic is either 0 or a prime number.

2.4 Factorization in integral domains

Lemma. A principal ideal (r) is a prime ideal in R if and only if $r = 0$ or r is prime.

Lemma. Let $r \in R$ be prime. Then it is irreducible.

Proposition. Let R be a Euclidean domain. Then R is a principal ideal domain.

Lemma. Let R be a principal ideal domain. If $p \in R$ is irreducible, then it is prime.

Lemma. Let R be a principal ideal domain. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be a chain of ideals. Then there is some $N \in \mathbb{N}$ such that $I_n = I_{n+1}$ for some $n \geq N$.

Proposition. Let R be a principal ideal domain. Then R is a unique factorization domain.

Lemma. Let R be a unique factorization domain. Then greatest common divisors exists, and is unique up to associates.

2.5 Factorization in polynomial rings

Lemma (Gauss' lemma)**.** Let R be a UFD, and $f \in R[X]$ be a primitive polynomial. Then f is reducible in $R[X]$ if and only if f is reducible $F[X]$, where F is the field of fractions of R.

Lemma. Let R be a UFD. If $f, g \in R[X]$ are primitive, then so is fg.

Corollary. Let R be a UFD. Then for $f, g \in R[X]$, we have that $c(fg)$ is an associate of $c(f)c(g)$.

Lemma (Gauss' lemma)**.** Let R be a UFD, and $f \in R[X]$ be a primitive polynomial. Then f is reducible in $R[X]$ if and only if f is reducible $F[X]$, where F is the field of fractions of R.

Proposition. Let R be a UFD, and F be its field of fractions. Let $g \in R[X]$ be primitive. We let

$$J = (g) \lhd R[X], \quad I = (g) \lhd F[X].$$

Then

$$J = I \cap R[X].$$

In other words, if $f \in R[X]$ and we can write it as $f = gh$, with $h \in F[X]$, then in fact $h \in R[X]$.

Theorem. If R is a UFD, then $R[X]$ is a UFD.

Proposition (Eisenstein's criterion)**.** Let R be a UFD, and let

$$f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$$

be primitive with $a_n \neq 0$. Let $p \in R$ be irreducible (hence prime) be such that

(i) $p \nmid a_n$;

(ii) $p \mid a_i$ for all $0 \leq i < n$;

(iii) $p^2 \nmid a_0$.

Then f is irreducible in $R[X]$, and hence in $F[X]$ (where F is the field of fractions of F).

2.6 Gaussian integers

Proposition. A prime number $p \in \mathbb{Z}$ is prime in $\mathbb{Z}[i]$ if and only if $p \neq a^2 + b^2$ for $a, b \in \mathbb{Z} \setminus \{0\}$.

Lemma. Let p be a prime number. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field with p elements. Let $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ be the group of invertible elements under multiplication. Then $\mathbb{F}_p^\times \cong C_{p-1}$.

Proposition. The primes in $\mathbb{Z}[i]$ are, up to associates,

(i) Prime numbers $p \in \mathbb{Z} \leq \mathbb{Z}[i]$ such that $p \equiv 3 \pmod 4$.

(ii) Gaussian integers $z \in \mathbb{Z}[i]$ with $N(z) = z\bar{z} = p$ for some prime p such that $p = 2$ or $p \equiv 1 \pmod 4$.

Corollary. An integer $n \in \mathbb{Z}_{\geq 0}$ may be written as $x^2 + y^2$ (as the sum of two squares) if and only if "when we write $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ as a product as distinct primes, then $p_i \equiv 3 \pmod 4$ implies n_i is even".

2.7 Algebraic integers

Proposition. Let $\alpha \in \mathbb{C}$ be an algebraic integer. Then the ideal

$$I = \ker(\phi : \mathbb{Z}[X] \to \mathbb{C}, f \mapsto f(\alpha))$$

is principal, and equal to (f_α) for some irreducible monic f_α.

Lemma. Let $\alpha \in \mathbb{Q}$ be an algebraic integer. Then $\alpha \in \mathbb{Z}$.

2.8 Noetherian rings

Proposition. A ring is Noetherian if and only if every ideal is finitely generated.

Proposition. Let R be a Noetherian ring and I be an ideal of R. Then R/I is Noetherian.

Theorem (Hilbert basis theorem)**.** Let R be a Noetherian ring. Then so is $R[X]$.

3 Modules

3.1 Definitions and examples

Theorem (First isomorphism theorem)**.** Let $f : M \to N$ be an R-module homomorphism. Then

$$\ker f = \{m \in M : f(m) = 0\} \leq M$$

is an R-submodule of M. Similarly,

$$\operatorname{im} f = \{f(m) : m \in M\} \leq N$$

is an R-submodule of N. Then

$$\frac{M}{\ker f} \cong \operatorname{im} f.$$

Theorem (Second isomorphism theorem)**.** Let $A, B \leq M$. Then

$$A + B = \{m \in M : m = a + b \text{ for some } a \in A, b \in B\} \leq M,$$

and

$$A \cap B \leq M.$$

We then have

$$\frac{A + B}{A} \cong \frac{B}{A \cap B}.$$

Theorem (Third isomorphism theorem)**.** Let $N \leq L \leq M$. Then we have

$$\frac{M}{L} \cong \left(\frac{M}{N}\right) / \left(\frac{L}{N}\right).$$

Lemma. An R-module M is finitely-generated if and only if there is a surjective R-module homomorphism $f : R^k \twoheadrightarrow M$ for some finite k.

Corollary. Let $N \leq M$ and M be finitely-generated. Then M/N is also finitely generated.

3.2 Direct sums and free modules

Proposition. For a subset $S = \{m_1, \cdots, m_k\} \subseteq M$, the following are equivalent:

(i) S generates M freely.

(ii) S generates M and the set S is independent.

(iii) Every element of M is *uniquely* expressible as

$$r_1 m_1 + r_2 m_2 + \cdots + r_k m_k$$

for some $r_i \in R$.

Proposition (Invariance of dimension/rank)**.** Let R be a non-zero ring. If $R^n \cong R^m$ as R-modules, then $n = m$.

Proposition. If $I \lhd R$ is an ideal and M is an R-module, then M/IM is an R/I module in a natural way.

Proposition. Every non-zero ring has a maximal ideal.

Proposition (Invariance of dimension/rank)**.** Let R be a non-zero ring. If $R^n \cong R^m$ as R-modules, then $n = m$.

3.3 Matrices over Euclidean domains

Theorem (Smith normal form)**.** An $m \times n$ matrix over a Euclidean domain R is equivalent to a diagonal matrix

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix},$$

with the d_i all non-zero and

$$d_1 \mid d_2 \mid d_3 \mid \cdots \mid d_r.$$

Lemma. Let A and B be equivalent matrices. Then

$$\mathrm{Fit}_k(A) = \mathrm{Fit}_k(B)$$

for all k.

Corollary. If A has Smith normal form

$$B = \begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix},$$

then

$$\mathrm{Fit}_k(A) = (d_1 d_2 \cdots d_k).$$

So d_k is unique up to associates.

Lemma. Let R be a principal ideal domain. Then any submodule of R^m is generated by at most m elements.

Theorem. Let R be a Euclidean domain, and let $N \leq R^m$ be a submodule. Then there exists a basis $v_1, \cdots, v_m$ of R^m such that N is generated by $d_1 v_1, d_2 v_2, \cdots, d_r v_r$ for some $0 \leq r \leq m$ and some $d_i \in R$ such that

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Corollary. Let R be a Euclidean domain. A submodule of R^m is free of rank at most m. In other words, the submodule of a free module is free, and of a smaller (or equal) rank.

Theorem (Classification of finitely-generated modules over a Euclidean domain)**.** Let R be a Euclidean domain, and M be a finitely generated R-module. Then

$$M \cong \frac{R}{(d_1)} \oplus \frac{R}{(d_1)} \oplus \cdots \oplus \frac{R}{(d_r)} \oplus R \oplus R \oplus \cdots \oplus R$$

for some $d_i \neq 0$, and

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Corollary (Classification of finitely-generated abelian groups)**.** Any finitely-generated abelian group is isomorphic to

$$C_{d_1} \times \cdots \times C_{d_r} \times C_\infty \times \cdots \times C_\infty,$$

where $C_\infty \cong \mathbb{Z}$ is the infinite cyclic group, with

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Corollary. If A is a finite abelian group, then

$$A \cong C_{d_1} \times \cdots \times C_{d_r},$$

with

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Lemma (Chinese remainder theorem)**.** Let R be a Euclidean domain, and $a, b \in R$ be such that $\gcd(a, b) = 1$. Then

$$\frac{R}{(ab)} \cong \frac{R}{(a)} \times \frac{R}{(b)}$$

as R-modules.

Theorem (Prime decomposition theorem)**.** Let R be a Euclidean domain, and M be a finitely-generated R-module. Then

$$M \cong N_1 \oplus N_2 \oplus \cdots \oplus N_t,$$

where each N_i is either R or is $R/(p^n)$ for some prime $p \in R$ and some $n \geq 1$.

3.4 Modules over $\mathbb{F}[X]$ and normal forms for matrices

Lemma. If V is a finite-dimensional vector space, then V_α is a finitely-generated $\mathbb{F}[X]$-module.

Theorem (Rational canonical form)**.** Let $\alpha : V \to V$ be a linear endomorphism of a finite-dimensional vector space over $\mathbb{F}$, and V_α be the associated $\mathbb{F}[X]$-module. Then

$$V_\alpha \cong \frac{\mathbb{F}[X]}{(f_1)} \oplus \frac{\mathbb{F}[X]}{(f_2)} \oplus \cdots \oplus \frac{\mathbb{F}[X]}{(f_s)},$$

with $f_1 \mid f_2 \mid \cdots \mid f_s$. Thus there is a basis for V in which the matrix for α is the block diagonal

$$\begin{pmatrix} c(f_1) & 0 & \cdots & 0 \\ 0 & c(f_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & c(f_s) \end{pmatrix}$$

Lemma. The prime elements of $\mathbb{C}[X]$ are the $X - \lambda$ for $\lambda \in \mathbb{C}$ (up to multiplication by units).

Theorem (Jordan normal form)**.** Let $\alpha : V \to V$ be an endomorphism of a vector space V over $\mathbb{C}$, and V_α be the associated $\mathbb{C}[X]$-module. Then

$$V_\alpha \cong \frac{\mathbb{C}[X]}{((X-\lambda_1)^{a_1})} \oplus \frac{\mathbb{C}[X]}{((X-\lambda_2)^{a_2})} \oplus \cdots \oplus \frac{\mathbb{C}[X]}{((X-\lambda_t)^{a_t})},$$

where $\lambda_i \in \mathbb{C}$ do *not* have to be distinct. So there is a basis of V in which α has matrix

$$\begin{pmatrix} J_{a_1}(\lambda_1) & & & 0 \\ & J_{a_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & J_{a_t}(\lambda_t) \end{pmatrix},$$

where

$$J_m(\lambda) = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda \end{pmatrix}$$

is an $m \times m$ matrix.

Theorem (Cayley-Hamilton theorem)**.** Let M be a finitely-generated R-module, where R is some commutative ring. Let $\alpha : M \to M$ be an R-module homomorphism. Let A be a matrix representation of α under some choice of generators, and let $p(t) = \det(tI - A)$. Then $p(\alpha) = 0$.

3.5 Conjugacy of matrices*

Lemma. Let $\alpha, \beta : V \to V$ be two linear maps. Then $V_\alpha \cong V_\beta$ as $\mathbb{F}[X]$-modules if and only if α and β are conjugate as linear maps, i.e. there is some $\gamma : V \to V$ such that $\alpha = \gamma^{-1}\beta\gamma = \alpha$.

Corollary. There is a bijection between conjugacy classes of $n \times n$ matrices over $\mathbb{F}$ and sequences of monic polynomials $d_1, \cdots, d_r$ such that $d_1 \mid d_2 \mid \cdots \mid d_r$ and $\deg(d_1, \cdots, d_r) = n$.