UNIVERSITY OF TORONTO, DEPARTMENT OF MATHEMATICS

MAT1100 Summary of major results

Xin Qi

December 13, 2014

This is a summary of the major results we covered over the course. A few proofs are also included.

CONTENTS

1 Groups **2**
- 1.1 Basic results in groups 2
- 1.2 Sylow Theorems 4
- 1.3 Semi-direct products 4

2 Rings **5**
- 2.1 Basic results of rings 5
- 2.2 UFDs, PIDs, Euclidean Domains 5

3 Modules **6**
- 3.1 Basic results of modules 6
- 3.2 Tensor products 7

4 Localization and fields of fractions **7**

1 GROUPS

1.1 BASIC RESULTS IN GROUPS

Definition 1.1. Let G be a group, $g, h \in G$. Conjugation of g by h (g^h) is the element $h^{-1}gh$.

Definition 1.2. Let G be a group, $N < G$. N is a normal subgroup of G ($N \lhd G$) if for every $g \in G$, $N^g = \{g^{-1}ng : n \in N\} = N$.

Remark 1.3.

- Every $N \lhd G$ is the kernel of some surjective homomorphism $\varphi : G \to H$. (Construct an equivalence relation on elements of G, $g_1 \; g_2$ if $g_1^{-1}g_2 \in N$, let $H = G/$ and do the natural thing.)
- For any $K < G$, $|K| \mid |G|$.

Theorem 1.4. First Isomorphism Theorem $\phi : G \to H$ *is a group homomorphism then* $G/\ker(\phi) \cong im(\phi)$.

Proof. Define $R : G/\ker(\phi) \to im(\phi)$ by $R([g]) = \phi(g)$ and check it is well-defined. Define $L : im(\phi) \to G/\ker(\phi)$ by $L(h) = [g]$ and check that it is also well-defined. Show the two maps are homomorphism and the two compositions are identities. □

Remark 1.5. $H, K < G$. $HK = \{hk : h \in H, k \in K\}$. $HK < G \Leftrightarrow HK = KH$.

Definition 1.6. G is a group, X a subset of G.

- Normalizer: $N_G(X) = \{g \in G : X^g = X\}$
- Centralizer: $C_G(X) = \{g \in G : \forall x \in X, gx = xg\} = \{g \in G : \forall x \in X, x^g = x\}$
- Center: $Z(G) = C_G(G)$

Proposition 1.7. *If* $H < H_G(K)$ *then* $HK = KH$, $K \lhd HK$, *and* $H \bigcap K \lhd H$.

Proof.

- $H < N_G(K)$, so $\forall h \in H$, $hK = Kh$. Then $\bigcup_{h\in H} hK = HK$ and $\bigcup_{h\in H} Kh = KH$. Thus $HK = KH$ (consequently a group).
- $K^{hk} = (K^h)^k = K^k = K$
- $a \in H \bigcap K$ then $a^h \in H^h = H$, $a^h \in K^h = K$. So $a^h \in H \bigcap K$.

□

Theorem 1.8. Second Isomorphism Theorem for Groups G *is a group,* $H, K < G$, $H < N_G(K)$. *Then* $HK/K \cong H/H \bigcap K$.

Proof. Define $R : HK/K \to H/H\bigcap K$, $R([hk]_K) = [h]_{H\bigcap K}$. It's well-defined, consider $h_1k_1 \; h_2k_2$, so $h_1k_1k' = h_2k_2$. We want $[h_1]_{H\bigcap K} = [h_2]_{H\bigcap K}$, equivalently $h_1^{-1}h_2 \in H\bigcap K$. Well $h_1^{-1}h_2 \in H$, and $h_1k_1k'k_2^{-1} = h_2$, so $h_1^{-1}h_2 = h_1^{-1}h_1k_1k'k_2^{-1} = k_1k'k_2^{-1} \in K$. Define $L : H/H\bigcap K \to HK/K$, $L([h]_{H\bigcap K}) = [h]_K$. It's well-defined since $H\bigcap K \subseteq K$. Check that R, L are multiplicative and inverses of each other. □

Theorem 1.9. Third Isomorphism Theorem for Groups *G is a group, $H, K \lhd G$, $K < H$. Then $\frac{G/K}{H/K} \cong G/H$. In particular $H/K \lhd G/K$.*

Proof. Define $R : \frac{G/K}{H/K} \to G/H$, $R([[g]_K]_{H/K}) = [g]_H$. Define $L : G/H \to \frac{G/K}{H/K}$, $L([g]_H) = [[g]_K]_{H/K}$. Check they are well-defined, multiplicative, and inverses of each other. □

Theorem 1.10. Fourth Isomorphism Theorem for Groups *G is a group, $N \lhd G$. Then $\pi : G \to G/H$ induces a faithful bijection between subgroups $\{H : N < H < G\}$ and subgroups of G/N. Faithfully means $N < A < B < G$ implies $\pi(A) < \pi(B)$, $A \lhd B$ implies $\pi(A) \lhd \pi(B)$, and $\pi(A \bigcap B) = \pi(A) \bigcap \pi(B)$.*

Definition 1.11. A nontrivial group G is simple if the only subgroups of G are G and $\{1\}$.

Proposition 1.12. *$\mathbb{Z}/n$ is simple $\Leftrightarrow$ n is prime.*

Theorem 1.13. Jordan-Hölder *Let G be a finite group then there exists a sequence of the following form:*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$$

such that $H_i = G_i/G_{i+1}$ is simple, and the sequence of H_i's (called the composition series of G) is unique up to a permutation.

Remark 1.14. You cannot reconstruct G from the H_i's.

Definition 1.15. Given, $\sigma \in S_n$, the sign of σ is the parity of the number of transpositions required to write σ as a product of those transpositions.

Corollary 1.16.

- *σ and σ' are conjugates if and only if they have the same list of cycle lengths.*
- *The number of conjugacy classes in S_n is the number of partitions of n.*

Theorem 1.17. *$A_n \lhd S_n$ is simple for $n = 3$ or $n \geq 5$.*

Definition 1.18. Given a group G, a (left) G-Set is a set X along with a (left) action of G on X i.e. a map $\bullet : G \times X \to X$ such that

1. $\forall x \in X$, $1_G \bullet x = x$
2. $\forall g_1, g_2 \in G$, $\forall x \in X$, $g_1 \bullet (g_2 \bullet x) = (g_1 g_2) \bullet x$

Definition 1.19.

- A G-Set is transitive if $\forall x, y \in X$, there exist $g \in G$ such that $g \bullet x = y$.
- $\text{Stab}_X(x) = g \in G : gx = x$
- The orbit of $x \in X$ is Gx.

Theorem 1.20.

1. *Every G-Set is a disjoint union of transitive G-Sets.*
2. *if X is a transitive G-Set, then $X \cong G/Stab_X(x)$ with $x \in X$/.*

Theorem 1.21. *If X is a G-Set, and x_i are representatives of the orbits of X, then $|X| = \sum_i |Gx_1| = \sum_i \frac{|G|}{|Stab_X(x_i)|}$. ($X$, G finite).*

Corollary 1.22. *In the case where G acts on itself by conjugation, then G equals the union of the conjugacy classes. Let y_i be the representatives of the conjugacy classes of size greater than 1, then we have the class equation:*

$$|G| = |Z(G)| + \sum_i \frac{|G|}{|C_G(y_i)|}$$

Theorem 1.23. *If G is a group of order p^α, where p is prime then $Z(G)$ is nontrivial.*

Proof. Look at the class equation and conclude that $|Z(G)|$ is divisible by p. □

1.2 Sylow Theorems

For this subsection, G is finite, p is prime, $|G| = p^\alpha m$ where $p \nmid m$.

Definition 1.24. $Syl_p(G) = \{P < G : |P| = p^\alpha\}$

Lemma 1.25. Cauchy's Theorem *If G is a finite Abelian group of order divisible by p, then G contains an element of order p.*

Theorem 1.26. Sylow theorems 1-3

1. *$Syl_p(G) \neq \emptyset$*
2. *Every p-subgroup (subgroup of G with order of every element being a power of p) of G is contained in some Sylow-p subgroup of G.*
3. *All Sylow-p subgroups of G are conjugate. Define $n_p(G) := |Syl_p(G)|$, then $n_p(G) \mid |G|$ and $n_p(G) = 1 \mod p$.*

Remark 1.27. A group of order p is isomorphic to $\mathbb{Z}/p$.

Remark 1.28. If $\gcd(a, b) = 1$ then $\mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/ab$.

1.3 Semi-direct products

Given $N, H < G$, we want to compare $N \times H$ with NH. There is always a map $\mu : N \times H \to NH$ but in general there is not much to be said about μ.

Definition 1.29. If N, H are arbitrary groups, and $\phi : H \to Aut(N)$ is a homomorphism. Denote the semi-direct product of N and H relative to ϕ as $N \rtimes_\phi H$. Where $N \rtimes_\phi H = \{nh : n \in N, h \in H\}$ with the product $(n_1 h_1)(n_2 h_2) = (n_1 \phi_{h_1}(n_2) n_2)(h_1 h_2)$

Proposition 1.30.

1. *$N \rtimes H$ is indeed a subgroup with $e_{N \rtimes H} = e_N e_H = e$*
2. *$H < N \rtimes H$*
3. *$N \lhd N \rtimes H$, $N \rtimes H / N \cong H$*
4. *$N \bigcap H = e$, $n^{h^{-1}} = \phi_h(n)$*

Theorem 1.31. *If $G = NH$, $N \lhd G$, $H < G$, $H \bigcap N = e$, then $G \cong N \rtimes_\phi H$ where $\phi_h(n) = n^h$*

2 RINGS

2.1 BASIC RESULTS OF RINGS

Remark 2.1. The evaluation map ($ev_u : R[x] \to R$), is a ring homomorphism provided R is commutative.

Theorem 2.2. Cayley-Hamilton *A matrix annihilates its characteristic polynomial. Let A be a $n \times n$ matrix over a commutative ring R, let χ_A be the characteristic polynomial of A ($\chi_A(t) = \det(tI - A)$), then $\chi_A(A) = 0$.*

Definition 2.3. An ideal I of a ring R is proper if $I \neq R \Leftrightarrow 1 \notin I$.

Remark 2.4. Every proper ideal is the kernel of some ring homomorphism.

Theorem 2.5. Ring Isomorphism Theorems 1-4

1. *$\varphi : R \to S$ a ring homomorphism, then $R/\ker(\varphi) \cong im(\varphi)$.*
2. *A is a subring of R, I an proper ideal, then $\frac{A+I}{I} = \frac{A}{A \cap I}$.*
3. *$I \subset J \subset R$ are proper ideals, then $\frac{R/I}{J/I} \cong R/J$.*
4. *Given a proper ideal I of R, there is a bijection between ideals J where $I \subset J \subset R$ and ideals of R/I.*

From now on R is commutative.

Theorem 2.6. *$I \subset R$ is maximal $\Leftrightarrow$ R/I is a field.*

Theorem 2.7. *Every proper ideal in any ring is contained in a maximal ideal.*

Proposition 2.8. *R/I is a field $\Leftrightarrow$ I is maximal.*

Theorem 2.9. *A maximal ideal is prime.*

2.2 UFDs, PIDs, EUCLIDEAN DOMAINS

From now on R is commutative and a domain.

Definition 2.10. $a, b \in R$ are associates ($a\ b$) if $a \mid b$ and $b \mid a$.

Proposition 2.11. *If q, q' are both gcd of a and b, then $q\ q'$*

Definition 2.12.

- Given $x \notin R^\times, x \neq 0$, x is irreducible if $x = ab \Rightarrow a \in R^\times$ or $b \in R^\times$.
- Given $p \notin R^\times, x \neq 0$, p is prime if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Proposition 2.13. *p is prime implies p is irreducible.*

Theorem 2.14. *Given a UFD R, $x \in R \backslash 0$ can be written as a product of primes and a unit i.e. $x = up_1 \ldots p_n$, and this factorization is unique up to a permutation and units.*

Proposition 2.15. *In a UFD, x is prime if and only if x is irreducible.*

Proposition 2.16. *R is a UFD if and only if every nonzero $x \in R$ has a unqiue decomposition into irreducibles.*

Theorem 2.17. *gcd always exists in UFDs.*

Theorem 2.18. *We have the following chain of implications: R is an Euclidean domain $\Rightarrow$ R is a PID $\Rightarrow$ R is a UFD.*

Proposition 2.19. *A PID is Noetherian, that is every descending sequence of ideals in R is eventually constant.*

Proposition 2.20. *In a PID, $< a, b >=< \gcd(a, b) >$.*

Definition 2.21. A Dedekind-Hasse (D-H) norm on R is a function $d : R \backslash \{0\} \to \mathbb{N}_{>0}$ such that if $a, b \neq 0$, either $b \mid a$ or there exist $x \in < a, b > \backslash 0$ with $d(x) < d(a)$.

Theorem 2.22. *R is a PID $\Leftrightarrow$ it has a D-H norm.*

Theorem 2.23. *Let R be an UFD, $g = gcd(a, b)$, $l = lcm(a, b)$, $l = \frac{ab}{g}$. If $g = sa + tb$ (guaranteed in a PID) then*

$$R/ < a > \oplus R/ < b > \cong R/ < g > \oplus R/ < l >$$

In particular, if $g = 1$, $l = ab$, then $R/ < a > \oplus R/ < b > \cong R/ < ab >$

3 Modules

3.1 Basic results of modules

Definition 3.1. A module M over a ring R is a set M with $0 \in M$, $+ : M \times M \to M$, $\bullet : R \times M \to M$ such that

1. $(M, +, 0)$ is an Abelian group.
2. $1m = m$, $a(bm) = (ab)m$.
3. $(a + b)m = am + bm$, $a(m + n) = am + an$.

Given a submodule N of M, we have M/N where m_1 m_2 if $m_1 - m_2 \in N$.

Theorem 3.2. Modules Isomorphism Theorem 1-4

1. *Given $\varphi : M \to N$, $M/\ker(\varphi) \cong im(\varphi)$.*
2. *$A, B \subset M$, $\frac{A+B}{B} \cong \frac{A}{A \bigcap B}$*
3. *$A \subset B \subset M$, $\frac{M/A}{B/A} \cong M/B$*
4. *Given a submodule N of M, there is a bijection between ideals J where $N \subset J \subset M$ and ideals of M/N.*

Theorem 3.3. Structure theorem for finitely generated modules over a PID *If M is a finitely generated module over a PID R, then*

$$M \cong R^k \oplus \bigoplus_{i=1}^{n} R/ < p_i^{s_i} >$$

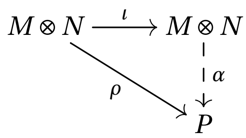
where the p_i are prime, $s_i \in \mathbb{Z}_{>0}$. Furthermore k is unique and the decomposition is unique up to an permutation of the $R/ < p_i^{s_i} >$'s.

Corollary 3.4. Jordan Normal Form *Over an algebraically closed field, every square matrix is conjugate to a matrix with Jordan blocks down the diagonal. Jordan blocks are blocks of the form:*

$$\begin{bmatrix} \lambda & 0 & \dots & \dots & \dots & 0 \\ 1 & \lambda & \ddots & & & \vdots \\ 0 & 1 & \lambda & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 & \lambda \end{bmatrix}$$

3.2 Tensor products

Definition 3.5. Given two R-modules M, N, we define the tensor product $M \otimes N$ to be a module along with a bilinear map $\iota : M \times N \to M \otimes N$ such that the following diagram commute:



That is, given any map ρ from $M \times N$ to P, there exist a unique map α from $M \otimes N$ to P such that $\rho = \alpha\iota$.

Theorem 3.6. *$M \otimes N$ exists and is unique up to an isomorphism.*

4 Localization and fields of fractions

Definition 4.1. R is a domain, $S \subset R \backslash \{0\}$ is multiplicative if $1 \in S$, and $s_1, s_2 \in S$ implies $s_1 s_2 \in S$.

Definition 4.2. Define $S^{-1}R := \{\frac{r}{s} : r \in R, s \in S\}/(s_2 r_1 = s_1 r2, 0 = \frac{0}{1}, 1 = \frac{1}{1}, \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \frac{a}{b}\frac{c}{d} = \frac{ac}{bd})$. $S^{-1}R$ is called the localization of R at S.