

# Math H113 - Spring 2014 Notes

April 8, 2014

## Introduction

This is a sparse collection of facts taken from Dummit and Foote, 3e. The goal is to recap the most important things Prof. Vojta has covered, with an emphasis on non-obvious results.

## Chapter 0/1

1. gcd:  $(m, n) = am + bn$ .
2. The Euler function:  $\varphi(p^a) = p^{a-1}(p-1)$ ,  $\varphi(ab) = \varphi(a)\varphi(b)$  if  $(a, b) = 1$ .
3. The dihedral group:  $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ .
4. Fields  $(F, F^\times = F - \{0\})$ :  $(F, +)$  and  $(F^\times, \times)$  are abelian groups. Note: if  $|F| < \infty$ ,  $\exists p, m$  s.t.  $|F| = p^m$ .
5. Symmetries:  $|S_n| = n!$ . Disjoint cycles commute, but  $S_{n \geq 3}$  is non-abelian.
6. Group actions on  $A$  by  $G$ : (i)  $g_1(g_2a) = (g_1g_2)a$ , (ii)  $1a = a$ .  $\forall g_1, g_2, a$ .
  - (a) Fixing  $g \in G$  in the action gives  $\sigma_g \in S_A$ .
  - (b)  $g \mapsto \sigma_g$  is a homomorphism ( $G \rightarrow S_A$ , the permutation representation).

## Chapter 2

1. Subgroup criterion:  $H \neq \phi$  and  $xy^{-1} \in H \forall x, y \in H$ .
2. Centralizer:  $\leq G$ , commutes with  $A$ . Center:  $\leq G$ , commutes with  $G$  itself.
3. Normalizer:  $\leq G$  s.t.  $gAg^{-1} = A \forall g$ .
4. Stabilizer: fixing  $a \in A$ ,  $\leq G$  s.t.  $ga = a$ . Kernel:  $\forall a \in A$ ,  $\leq G$  s.t.  $ga = a$ .
5. If  $x^m = 1$  and  $x^n = 1$ ,  $x^{(m,n)} = 1$  (in cyclic groups).

6. Let  $x \in G$ ,  $a \neq 0$ : if  $|x| = \infty$  then  $|x^a| = \infty$ . Else, if  $|x| = n$ , then  $|x^a| = n/(n, a)$  ( $\star$ ).
7. Every subgroup of a cyclic group is cyclic, and cyclic groups of the same order are isomorphic to each other.
8. Let  $|x| = n$ ,  $H = \langle x \rangle$ . Only if  $(n, a) = 1$ ,  $H = \langle x^a \rangle$  (count these with  $\varphi(n)$ ).  
A general statement:  $\langle x^m \rangle = \langle x^{(n, m)} \rangle$ .
9. Let  $A \neq \phi$  be a set of subgroups of  $G$ . Then their intersection  $\langle A \rangle = \cap A \leq G$ .

## Chapter 3

1. Given  $\varphi : G \rightarrow H$ ;  $\varphi(1_G) = 1_H$ ,  $\ker \varphi \leq G$ , and  $\text{im}(\varphi) \varphi \leq H$ .
2.  $G/K$  is basically arithmetic on the fibers of  $\varphi$ , which are all cosets of  $\ker \varphi$ .
3. The set of left cosets of any  $N \leq G$  partitions  $G$ . However, the operation  $uN \cdot vN = (uv)N$  is only well defined if  $N \trianglelefteq G$  (or equivalently  $N_G(N) = G$ ,  $gN = Ng \ \forall g$ , or  $gNg^{-1} \subseteq N \ \forall g$ ).<sup>1</sup>
4. **Lagrange's Theorem:**  
If  $|G| < \infty$  and  $H \leq G$ , then  $|H| \mid |G|$  and  $|G : H| = |G|/|H|$
5. **Cauchy's Theorem:**  
If  $|G| < \infty$  and prime  $p \mid |G|$ ,  $\exists x \in G$  s.t  $|x| = p$ .
6. **Sylow's Theorem:**  
If  $|G| = p^\alpha m$  ( $p \nmid m$ ),  $\exists H \leq G$  s.t  $|H| = p^\alpha$ .
7.  $\ker \varphi \trianglelefteq G$ ,  $G/\ker \varphi \cong \varphi(G)$ ,  $\varphi$  is 1-1 iff  $\ker \varphi = 1$ , and  $|G : \ker \varphi| = |\varphi(G)|$ .
8. If finite  $H, K \leq G$ , then  $|HK| = \frac{|H||K|}{|H \cap K|}$ .  $HK \leq G$  only if  $KH \leq G$ .
9. Let  $A, B \leq G$  and  $A \leq N_G(B)$ . Then  $AB \leq G$ ,  $B \trianglelefteq AB$ ,  $A \cap B \trianglelefteq A$ , and  $AB/B \cong A/(A \cap B)$ .
10. Let  $H \leq K$  and  $H, K \trianglelefteq G$ : then  $K/H \trianglelefteq G/H$  so  $(G/H)/(K/H) \cong G/K$ .
11. For  $N \trianglelefteq G$ , there is a bijection between subgroups of  $G$  containing  $N$  and subgroups of  $G/N$
12. To show that a homomorphism from  $\varphi : G/N \rightarrow H$  is well-defined, one must prove  $N \leq \ker \Phi$  (with  $\Phi : G \rightarrow H$ ).
13.  $(a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_2)$ . The sign of a permutation (i.e the parity of the number of 2-cycles  $\epsilon(\sigma) \in \{\pm 1\}$ <sup>2</sup>) is representation-independent.

<sup>1</sup>A useful theorem for later:  $gH = H$  iff  $g \in H$ .

<sup>2</sup>An  $m$ -cycle is composed of  $m-1$  transpositions, immediately giving  $\epsilon(\sigma) = \text{Parity}(m-1)$ .

14.  $\epsilon : S_n \rightarrow \{\pm 1\}$  is a surjective homomorphism.  $\ker \epsilon = A_n$ , the group of even permutations. Note  $S_n/A_n \cong \epsilon(S_n) = \{\pm 1\}$  and  $|A_n| = \frac{n!}{2}$ .
15. If  $G = MN$  with  $M, N \trianglelefteq G$  then:  $G/(M \cap N) \cong (G/M) \times (G/N)$
16. For  $H \trianglelefteq G$  and  $|G : H| = p$  prime, then for all  $K \leq G$ , either  $K \leq H$  or  $(G = HK$  and  $|K : K \cap H| = p)$
17. The commutator subgroup  $N = \langle x^{-1}y^{-1}xy | x, y \in G \rangle$  is normal, and  $G/N$  is always abelian.
18. “Normal in” relation NOT transitive:  $A \trianglelefteq B \wedge B \trianglelefteq C \not\Rightarrow A \trianglelefteq C$
19. In general,  $H \times (G/H) \not\cong G$

## Chapter 4

1.  $\sigma_g : A \rightarrow A$  ( $a \mapsto ga$ ), and  $\varphi : G \rightarrow S_A$  ( $g \mapsto \sigma_g$ ). Note: the kernel of the action  $\cap_{a \in A} G_a = \ker \varphi$ .<sup>3</sup>
2. For  $A \neq \phi$ , each action  $G \times A \rightarrow A$  is isomorphic to a homomorphism  $G \rightarrow S_A$ . Let  $a \sim b$  iff  $a = gb$  for some  $g \in G$ : then  $\sim$  partitions  $G$ , and the order of the equivalence class (i.e orbit) containing  $a$  is  $|G : G_a|$ .<sup>4</sup>
3. Elements in  $G$  effect the same permutation on  $A$  iff they’re in the same coset of the kernel of the action.
4. Let  $H \leq G$ ,  $A$  be the set of left cosets of  $H$  in  $G$ , and  $G$  act on  $A$  (with  $\pi_H : G \rightarrow S_A$ ). Then the action is transitive,  $G_{1H} = H$ , and  $\ker \pi_H = \cap_{x \in G} xHx^{-1}$  (giving the largest normal subgroup of  $G$  in  $H$ ).
5. If  $|G| = n$ ,  $G \cong H$  for some  $H \leq S_n$ . If  $p$  is the smallest prime s.t  $p|n$ , then any subgroup  $H \leq G$  s.t  $|G : H| = p$  is normal.

## Chapter 5

1. Given a direct product  $G_1 \times G_2 \times \dots \times G_n$ ,  $G_i \cong \langle (1, \dots, g_i, \dots, 1) \mid g_i \in G_i \rangle$   
5
2. **Invariant Factor Decomposition:** Let  $G = \langle A \rangle$  ( $A \subseteq G$ , finite). Then  $G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \dots \times Z_{n_s}$  s.t  $r \geq 0$ ,  $n_j \geq 2 \forall j$ , and  $n_{i+1} | n_i$  for  $1 \leq i < s$  uniquely (up to isomorphism).
3. **Elementary Divisor Decomposition:** Let  $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ . Then  $G \cong A_1 \times \dots \times A_k$  where  $|A_i| = p_i^{\alpha_i}$ . Each  $A_i \cong Z_{p_i^{\beta_1}} \times \dots \times Z_{p_i^{\beta_t}}$  where  $\beta_i \geq \beta_{i+1}$  and  $\sum_i^t \beta_i = \alpha_i$ .

<sup>3</sup>‘Faithful’ actions have kernels equal to  $\{1_G\}$

<sup>4</sup>‘Transitive’ actions induce only one orbit in  $A$ .

<sup>5</sup>The projection  $\pi : G \rightarrow G_i$  is  $g \mapsto g[i]$ .

4. Let  $n = \prod n_i$ : if  $p|n$  then  $p|n_1$ . If  $n$  is a product of distinct primes, then  $Z_n$  is the only abelian group of order  $n$  (up to isomorphism).
5. Full converse to Lagrange's Theorem: For any abelian group  $G$  of order  $n$ , there exists a subgroup of order  $k$  for all  $k|n$  (proof using decomposition theorems).
6.  $Z_m \times Z_n \cong Z_{mn}$  iff  $(m, n) = 1$ , so  $Z_n \cong Z_{p_1^{\alpha_1}} \times \dots \times Z_{p_k^{\alpha_k}}$ .
7. The group exponent is the smallest positive integer s.t.  $x^n = 1 \forall x \in G$ .
8. The elementary abelian group of order  $p^n$ :  $E_{p^n} = (Z_p)^n$ . Each non-identity element has order  $p$ , and there are  $p + 1$  subgroups of order  $p$  in  $E_{p^2}$ .

## Chapter 6

1. Let  $F(S)$  be the group of words formed from  $S$ . Given a map  $\psi : S \rightarrow G$ , there exists a unique homomorphism  $\Phi : F(S) \rightarrow G$  s.t.  $\Phi|_S = \psi$ .
2. Because  $\Phi$  is a homomorphism,  $\Phi(s_i^{\epsilon_i} \dots) = \psi(s_i)^{\epsilon_i} \dots$ .
3. Empty word:  $(1, 1, \dots)$ . Reduced word:  $s_{i+1} \neq s_i^{-1}$  and  $s_i = 1 \Rightarrow s_{k \geq i} = 1$ .
4. Subgroups of free groups are also free groups.
5. Let  $S \subseteq G$  s.t.  $G = \langle S \rangle$ . A presentation of  $G$  is some  $(S, R)$  s.t.  $\ker \Phi$  is the smallest normal subgroup containing  $\langle R \rangle$ .  $G$  is finitely generated if  $S$  is finite, and finitely presented if  $R$  is also finite.
6. Any free abelian group of rank  $n$  is  $\cong \mathbb{Z}^n$ .

## Chapter 7

1. Rings:  $(R, +)$  is abelian,  $\times$  is associative/distributive. If  $\times$  commutes, so does  $R$ . If  $1 \in R$ ,  $1r = r1 \forall r$ . If  $1 \neq 0$  and every nonzero element has an inverse,  $R$  is a division ring. Commutative division rings are fields.
2. Let  $a, b \in R$  be nonzero. Then  $a0 = 0a = 0$ . Zero divisors:  $ab = 0$  or  $ba = 0$ . The set of units (i.e.  $uv = vu = 1$ ) is  $R^\times$ .
3. Integral domains are commutative rings (with  $1 \neq 0$ ) with no zero divisors. Zero divisors cannot be units, therefore fields have no zero divisors.
4. Finite integral domains are fields. Subrings are  $\leq R$  and closed under  $\times$ .
5.  $R[x]$ :  $(ab)x^k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^k a_{k-i} b_i$ . Note:  $R \subset R[x]$  (as the constant polynomials) and  $R[x]$  is commutative iff  $R$  is.
6. If  $R$  is an integral domain,  $\deg(ab) = \deg(a) + \deg(b)$ ,  $R[x]^\times = R^\times$ , and  $R[x]$  is an integral domain.

7. Square matrices:  $(a_{ij}) \in M_n(R)$ . Invertible:  $GL_n(R)$ .
8. Fix a commutative ring  $R$  with  $1 \neq 0$  and let  $G$  be a finite group. Group rings  $RG$  contain all formal sums  $\sum_i r_i g_i$   $r_i \in R$ . Addition is done componentwise, and  $RG$  always has zero divisors.
9. Ring homomorphism:  $\varphi : R \rightarrow S$  s.t  $\varphi(a + b) = \varphi(a) + \varphi(b)$  and  $\varphi(ab) = \varphi(a)\varphi(b)$ .  $\ker \varphi = \{r \in R \mid \varphi(r) = 0_S\}$ , as if  $\varphi$  were a group homomorphism.
10.  $I = \ker \varphi$  is a subring of  $R$  (and an ideal/normal subgroup thereof),  $\text{im}(\varphi)$  is a subring of  $S$ . If  $\alpha \in \ker \varphi$ , then  $r\alpha, \alpha r \in R \forall r \in R$ .
11. Ideals: if  $rI \subseteq I$ ,  $Ir \subseteq I$ , and  $I$  subring of  $R$ .  $R/I$  is a quotient ring s.t  $(r+I) + (s+I) = (r+s)+I$  and  $(r+I) \times (s+I) = rs+I$ .  $R/\ker \varphi \cong \varphi(R)$ .  
Note: every ideal is the kernel of a ring homomorphism and vice versa.
12. Let  $A$  be a subring and  $B$  an ideal of  $R$ . Then  $A+B$  is a subring of  $R$ ,  $A \cap B$  is an ideal of  $A$ , and  $(A+B)/B \cong A/(A \cap B)$ .
13. Let  $I \subseteq J$  be ideals of  $R$ , then  $(R/I)/(J/I) \cong R/J$ .
14. For ideals  $I$  of  $R$ , there is a bijection between subrings of  $R$  containing  $I$  and subrings of  $R/I$
15. Ideal math:  $I + J = \{i + j \mid i \in I, j \in J\}$ ,  $IJ$  is the set of all finite sums of elements of the form  $ij$ , and  $I^n$  are all  $n$ -length products within  $I$ .
16.  $I + J$  is the smallest ideal containing  $I$  and  $J$ , and  $IJ \subseteq I \cap J$
17. If  $R$  is a commutative ring with a 1, and  $I + J = R$ , then  $IJ = I \cap J$