Math 401 - 01 Daily Topics - part 2 (Fall 2018)

$\newcommand{\aut}{\textrm{Aut}} \newcommand{\inn}{\textrm{Inn}} \newcommand{\sub}{\textrm{Sub}}
\newcommand{\cl}{\textrm{cl}} \newcommand{\join}{\vee} \newcommand{\bigjoin}{\bigvee}
\newcommand{\meet}{\wedge} \newcommand{\bigmeet}{\bigwedge} \newcommand{\normaleq}{\unlhd}
\newcommand{\normal}{\lhd} \newcommand{\union}{\cup} \newcommand{\intersection}{\cap}
\newcommand{\bigunion}{\bigcup} \newcommand{\bigintersection}{\bigcap} \newcommand{\sq}[2][\
]{\sqrt[#1]{#2\,}} \newcommand{\pbr}[1]{\langle #1\rangle} \newcommand{\ds}{\displaystyle}
\newcommand{\C}{\mathbb{C}} \newcommand{\R}{\mathbb{R}} \newcommand{\Q}{\mathbb{Q}}
\newcommand{\Z}{\mathbb{Z}} \newcommand{\N}{\mathbb{N}} \newcommand{\A}{\mathbb{A}}
\newcommand{\F}{\mathbb{F}} \newcommand{\T}{\mathbb{T}} \newcommand{\ol}[1]{\overline{#1}}
\newcommand{\imp}{\Rightarrow} \newcommand{\rimp}{\Leftarrow} \newcommand{\pinfty}{1/p^\infty}
\newcommand{\power}{\mathcal{P}} \newcommand{\calL}{\mathcal{L}} \newcommand{\calC}{\mathcal{C}}
\newcommand{\calN}{\mathcal{N}} \newcommand{\calB}{\mathcal{B}} \newcommand{\calF}{\mathcal{F}}
\newcommand{\calR}{\mathcal{R}} \newcommand{\calS}{\mathcal{S}} \newcommand{\calU}{\mathcal{U}}
\newcommand{\calT}{\mathcal{T}} \newcommand{\gal}{\textrm{Gal}} \newcommand{\isom}{\approx}
\newcommand{\idl}{\textrm{Idl}} \newcommand{\lub}{\textrm{lub}} \newcommand{\glb}{\textrm{glb}} $

Home

Week 7	Topics
10/01/2018	Test 1
10/02/2018	Lagrange's corollary 1
	Orbit-Stabilizer theorem
	Examples: cube, truncated icosahedron (soccer ball)
10/03/2018	Corollaries 2-5 to Lagrange's theorem
	Addendum to cor 3: moreover, there is a unique group of order p, up to isomorphism.
	Thm. 7.2
	Example 6, p.144
	Corollary: if p is the smallest prime divisor of $\|G\|$ and p^2 does not divide $\|G\|$, then G has at most one subgroup of index p (HW)
10/05/2018	Thm. 7.3

Week 8	Topics
10/08/2018	Test 1 returned and reviewed
	Prop: if $\varphi:G\to H$ is an isomorphism, then so is $\varphi^{-1}H\to G$.
	Prop: “isomorphic to” is an equivalence relation
	Thm. 6.1 Cayley's theorem
	$\aut(G)$, $\inn(G)$
10/09/2018	Thm 6.4 $\aut(G)$ is a group and $\inn(G)$ is a subgroup of $\aut(G)$
	Example: $\inn(D_4) \isom K_4$
	Prop: Let $G = <a>$ cyclic and H a group
	1. A homom $\varphi:G\to H$ is uniquely determined by $\varphi(a)$.
	2. If G has order n and $u\in H$ has order d where $d\|n$, then there is (unique) homomorphism $\varphi:G\to H$ s.t. $\varphi(a)=u$. Moreover, φ is injective iff $d=n$.

	3. If G has infinite order and $u\in H$, then there is (unique) homomorphism $\varphi:G\to H$ s.t. $\varphi(a)=u$. Moreover, φ is injective iff u has infinite order.
	Example: $\aut(\Z_n) \isom U_n$
10/10/2018	Board presentations PS 6
	Thms. 10.2 and 6.3
10/12/2018	Fall break

Week 9	Topics
10/15/2018	Prop. Let N \leq G. TFAE
	(i) $gNg^{-1} \subseteq N$ for all $g\in G$
	(ii) $gNg^{-1} = N$ for all $g\in G$
	(iii) $gN = Ng$ for all $g\in G$
	(iv) the product of any two left cosets is a left coset.
	Moreover, in the last one, we have $(gN)(hN) = ghN$
	Def: normal subgroup
	Examples: 1. $A_n \normaleq S_n$
	$<R_{360/n}> \normaleq D_n$
	Prop: if H is a subgroup of G of index 2, then H is a normal subgroup of G
	2. Prop: if $\varphi:G\to \bar{G}$ is a homomorphism, then $ker(\varphi)$ is a normal subgroup of G
	3. If G is abelian, then every subgroup of G is normal
	4. $Z(G)$ is a normal subgroup of G.
	5. G and $\{1\}$ are normal subgroups of G.
	Thm 9.2 proof using (iv) above.
	Example 9.10 Generalize $\Z/n\Z \isom \Z_n$
10/16/2018	Example 9.12
	Thm 10.3 1st Isom Thm
	Example $\varphi:\Z \to \Z_n$
	Thm 9.4
	Thm (N/C theorem) Let $H \leq G$. $N_G(H) / C_G(H)$ is isomorphic to a subgroup of $\aut(H)$.
10/17/2018	proof of N/C theorem
	Example 10.17 $\|G\|=35$
	Thm 9.3
	Corollary: If $\|G\|=pq$ and $Z(G) \neq 1$ then G is abelian.
	Thm 9.5 Cauchy's thm for abelian gps.
10/19/2018	Thm 10.4 $N\normaleq G$, $q:G \to G/N$ is an epimorphism with $ker(q)=N$
	Chapter 8 Direct Product
	Def: $G_1 \oplus G_2$
	Prop: 1) $G_1 \oplus G_2$ is a group.
	2) If G_1, G_2 are abelian then so is $G_1 \oplus G_2$.
	Examples: (1) $\Z_2 \oplus \Z_3$ is abelian of order 6, so it is isomorphic to $\Z_6$
	(2) $G \oplus \{1\} \isom G \isom \{1\}\oplus G$
	Cor: $G_1 \oplus G_2$ contains subgroups isomorphic to G_1 and G_2 respectively.
	Def: $G_1 \oplus \cdots \oplus G_n$
	Thm 8.1

Week 10	Topics
10/22/2018	Thm 8.2 G_1, G_2 finite. $G_1 \oplus G_2$ is cyclic iff G_1 and G_2 are cyclic or relatively prime orders.
10/23/2018	RSA cryptography. Public vs private keys

	Prop: $m^{ed}\equiv m \pmod n$.
	Internal direct product
	Thm.: Let $H,K\leq G$ be such that $HK=G$ and $H\intersection K=\{1\}$. Then $G\isom H\oplus K$.
	Def: When $H,K\leq G$ are such that $HK=G$ and $H\intersection K=\{1\}$, we say that G is the internal direct product of H and K, and write $G=H\times K$.
	Example: Consider D_n with $n=2m$ and m odd.
	Thm. 9.7 and corollary
	Prop: Let $H,N\leq G$.
	(1) If $N\normaleq G$ then $HN\leq G$.
	(2) If $H,N\normaleq G$ then $HN\normaleq G$
10/24/2018	2nd, 3rd, 4th and 5th isomorphism theorems.
	$\sub(D_4)$ and $\sub(V_4)$ as examples.
10/26/2018	Thm If G is a finite abelian group of order n, and $m\|n$ then G has a subgroup of order m.
	Fund. Thm. of Finite Abelian Groups
	Statement and examples, $n=12$ and $n=600$
	Elementary divisors form, and invariant factors form

Week 11	Topics
10/29/2018	Board presentations. Problems sets 7 and 8
10/30/2018	Ch.24 Def: conjugate, conjugate class $\cl(a)$.
	Prop: (1) “conjugate to” is an equivalence relation. The equivalence classes are the conjugacy classes.
	(2) $\cl(a)=\{a\} \iff a\in Z(G)$
	Thm. 24.1 without finite assumption
	Cor. 1
	Thm. Class equation (2 versions)
	Thm. 24.2 A non-trivial p-group has non-trivial center.
	Def: Finite p-group. Metabelian group.
	Cor. Let p be a prime. If $\|G\|=p^2$, then G is abelian.
	Cor. Let p be a prime. If $\|G\|=p^3$, then G is metabelian. Moreover, $\|Z(G)\|=p$ or $\|Z(G)\|=p^3$.
	Example: Heisenber group H has order p^3, and is not abelian.
10/31/2018	Thm. 24.3 Sylow's 1st Theorem
	Cor. Cauchy's theorem
	Cor. If $\|G\|=pq$ where $p<q$ are primes and $p\not\mid (q-1)$, then G is cyclic.
	Lemma 1. (1) Let $H\leq G$ and $C=\{gHg^{-1}\mid g\in G\}$ the set of all conjugates of H. Then $\|C\|=[G:N_G(H)]$.
	Definition of Sylow p-subgroup.
	(2) Let $H,K\leq G$. If $HK=KH$ then $HK\leq G$.
	Lemma 2. Let P be a Sylow p-subgroup G. If $g\in N_G(P)$ and $\|g\|$ is a power of p, then $g\in P$.
	Lemma 3. Let $\|G\|=p^km$ and $p\not\mid m$. Let P be a Sylow p-subgroup of G, i.e. $\|P\|=p^k$, and $H\leq G$ with $\|H\|=p^l$ for some $l\leq k$. Then there is a conjugate of P that contains H, i.e. there is $g\in G$ such that $H\leq gPg^{-1}$.
11/02/2018	Board presentations. Problems set 9
	Proof of Lemma3

Week 12	Topics
11/05/2018	Sylow Theorems
	Examples: (1) $\|G\|=35$ (2) $\|G\|=455$ (3) $\|G\|=21$ (4) $\|G\|=256$
11/06/2018	Test 2
11/07/2018	Rings. Definitions: ring, unity, ring with unity (unitary ring), commutative ring, units of a unitary ring
	Examples
	Prop: The units of a ring, $U(R)$ form a multiplicative group.

11/09/2018	No class.

Daily topics (3)

Home