Math 4120/6120, Summer 2020

Study guide: Midterm 1.

Note: This is just a guide, not an all-inclusive list.

Examples. One of the most helpful things that you can do in the beginning of the class is to *become very familiar with examples*, especially every group of order ≤ 12. There are not too many, and we've seen almost all of them. Of course, the only group of prime order p is $C_n \cong \mathbb{Z}_n$. Here is a complete list of those of non-prime order:

4. C_4, V_4
6. C_6, $D_3 \cong S_3$
8. C_8, $C_4 \times C_2$, C_2^3, D_4, Q_8
9. C_9, C_3^2
10. C_{10}, D_5
12. C_{12}, $C_6 \times C_2$, D_6, A_4, Dic_6.

In particular, for these groups (and for C_p), know their standard minimal generating set(s), be able to draw their Cayley diagrams, as well as their subgroup lattices. Know which subgroups are normal, and which subgroup is the center, $Z(G)$. For normal subgroups $N \lhd G$, be able to characterize the quotient, G/N. Be able to write presentations for these groups. Be able to express cyclic groups as $\mathbb{Z}_n$ (additively) or C_n (multiplicatively). Learn the seven frieze groups, their generators, Cayley diagrams, and presentations. It's also good to know *counterexamples* of things that aren't true; we've seen a few of these throughout the class.

Also familiarize yourself with a few common larger groups, such as S_4, A_5, S_5, and the integers $\mathbb{Z}$. Obviously, drawing the subgroup lattices of these would be too much to ask, but you should still be familiar with them and their subgroups, and know which are normal.

Permutations. You should be very comfortable composing permutations in cycle notation, computing their inverses, conjugacy classes, and recognizing whether they are even or odd. You should be familiar with the symmetric and alternating groups, and know standard generating sets for these groups.

Definitions. You will need to have the following basic formal definitions memorized.

(1) A *group* G. (The "official" definition.)
(2) A *left coset* xH of a subgroup $H \leq G$.
(3) A *normal subgroup* $H \lhd G$.
(4) The *index* $[G : H]$ of a subgroup $H \leq G$.
(5) The *direct product* $A \times B$ of two groups A and B.
(6) The *quotient* G/H of a group G by a normal subgroup $H \lhd G$.
(7) The *normalizer* $N_G(H)$ of a subgroup $H \leq G$.
(8) The *conjugacy class* $\mathrm{cl}_G(x)$ of an element $x \in G$.
(9) The *center* $Z(G)$ of a group.
(10) What it means for multiplication in G/N to be *well-defined*.

You should also be familiar with examples of the above concepts. For example, since $H \leq N_G(H) \leq G$, you should be able to come up with examples of when the normalizer is exactly H, when it is G, or when it is properly between these. Similarly, the center $Z(G)$ can contain one element, or the entire group, or something inbetween.

Useful facts and techniques.

(1) What Lagrange's theorem says about the a group's subgroups, and the relationship between $|G|$, $|H|$, and $[G : H]$.
(2) How to multiply elements (cosets!) in a quotient group, G/N.

(3) How to find the conjugacy class of an element $g \in G$.
(4) Two different ways to show that a subset $H \subseteq G$ is a subgroup.
(5) Three different ways to show that a subgroup $H \leq G$ is normal. Sometimes one is more useful than the others!
(6) How to find the normalizer of a subgroup.
(7) Two elements in S_n are conjugate iff they have the same cycle type.
(8) When showing equality of two *sets*, $A = B$, you need to show both $\subseteq$ and $\supseteq$.

Proofs to learn.

(1) Prove that the identity element of a group is unique.
(2) Prove that every element in a group has a unique inverse.
(3) Prove that if $\{H_\alpha \mid \alpha \in I\}$ is a collection of subgroups, then $\displaystyle\bigcap_{\alpha \in I} H_\alpha$ is a subgroup.
(4) Prove that $xH = H$ if and only if $x \in H$.
(5) Prove that if $[G : H] = 2$, then $H \lhd G$.
(6) The tower law: $[G : H][H : K] = [G : K]$.
(7) Prove that if $K \leq H \leq G$ and $K \lhd G$, then $K \lhd H$.
(8) Prove that the center $Z(G) = \{z \in G \mid gz = zg,\ \forall g \in G\}$ is a subgroup of G and that it is normal.
(9) Let $H \lhd G$. Prove that multiplication of cosets is well-defined: if $a_1H = a_2H$ and $b_1H = b_2H$, then $a_1H \cdot b_1H = a_2H \cdot b_2H$. Additionally, show that G/H is a group under this binary operation.
(10) Prove that if G is abelian and $H \leq G$, then G/H is abelian.
(11) Prove that the normalizer $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is a subgroup of G.
(12) Prove that $\mathrm{cl}_G(x) = \{x\}$ if and only if $x \in Z(G)$.

Study guide: Midterm 2.

Definitions to memorize.

(1) A *homomorphism* ϕ from a group G to a group H.
(2) An *isomorphism* ϕ from a group G to a group H.
(3) The *kernel* $\ker\phi$ of a homomorphism $\phi\colon G\to H$.
(4) What it means for a map $f\colon G/N\to H$ to be *well-defined*.
(5) The *commutator subgroup* G' of a group G, and the *abelianization* G/G'.
(6) A *group action* of G on a set S.
(7) The *orbit* of an element $s\in S$.
(8) The *stabilizer* of an element $s\in S$.
(9) The *fixed points* of a group action.
(10) A *p-group*, and a *Sylow p-subgroup* of a group G.

Useful facts and techniques.

(1) $\mathbb{Z}_n\times\mathbb{Z}_m$ iff $\gcd(n,m)=1$.
(2) Learn to classify all finite abelian groups of a fixed order.
(3) There are two ways to prove that $G/N\cong H$: Either construct a map $G/N\to H$ and prove it is a well-defined bijective homorphism, or construct a map $\phi\colon G\to H$ and prove it is an onto homomorphism with $\ker\phi=N$.
(4) Learn the statement of the Correspondence Theorem: There is a 1–1 correspondence between subgroup of G/N and subgroups of G that contain N. Moreover, every subgroup of G/N is of the form H/N for some $N\le H\le G$.
(5) Learn how to identify the commutator subgroup of G just from the subgroup lattice.
(6) $\mathrm{Aut}(\mathbb{Z}_n)\cong U_n$.
(7) The orbit-stabilizer theorem: If G acts on S, then $|G|=|\operatorname{Orb}(s)|\cdot|\operatorname{Stab}(s)|$ for any $s\in S$.
(8) Learn what the orbits, stabilizers, and fixed points are of the following actions:
  (i) G acting on itself by right multiplication.
  (ii) G acting on itself by conjugation.
  (iii) G acting on its subgroups by conjugation.
  (iv) G acting on its right cosets by right multiplication.
(9) Learn how to use the 3rd Sylow theorem to show that a group of a certain order is simple. (Usually, by showing that $n_p=1$ for some prime p.)

Proofs to learn.

(1) Let $\phi\colon G\to H$ be a homomorphism. Prove that $\phi(1_G)=1_H$, where 1_G and 1_H are the identity elements of G and H, respectively. Additionally, prove that $\phi(g^{-1})=\phi(g)^{-1}$ for all $g\in G$.
(2) Let $\phi\colon G\to H$ be a homomorphism. Prove that $\ker\phi:=\{k\in G\mid\phi(k)=1_H\}$ is a subgroup of G, and that it is normal.
(3) Prove that $A\times B\cong B\times A$.
(4) Prove that if $H\le G$, then $xHx^{-1}\cong H$ for any $x\in G$.
(5) Prove there is no embedding $\varphi\colon\mathbb{Z}_n\to\mathbb{Z}$.
(6) Prove that if $\varphi\colon G\to H$ is a homomorphism and $N\lhd H$, then $\varphi^{-1}(N)$ is a normal subgroup of G.
(7) If $H\le G$ is the only subgroup of G of order $|H|$, then H must be normal.
(8) The FHT: If $\varphi\colon G\to H$ is a homomorphism, then $G/\ker\varphi\cong\operatorname{im}\varphi$.
(9) The Diamond Isomorphism Theorem: If $A,B\lhd G$, then $AB\le G$, $B\lhd AB$, $(A\cap B)\lhd A$, and $AB/B\cong A/(A\cap B)$.
(10) Show that $\mathbb{Q}^*\cong\mathbb{Q}^+\times C_2$ and $\mathbb{Q}^*/\langle-1\rangle\cong\mathbb{Q}^+$, where $\mathbb{Q}^*$ is the nonzero rationals under multiplication, and $\mathbb{Q}^+\le\mathbb{Q}^*$ is the subgroup of positive rationals.
(11) Prove that G is abelian iff its commutator subroup $G'=\{e\}$.
(12) Prove that G/G' is abelian.

(13) Show that if G acts on S, then $\mathrm{Stab}(s)$ is a subgroup of G, for any $s \in S$.

(14) Prove that if G is a p-group, then $|Z(G)| > 1$. (Use the class equation.)

Study guide: Final exam.

Note: This is *in addition*, not instead, of the Midterm 1 and 2 material.

Definitions to memorize.

(1) A *field* F.
(2) A *field automorphism* of F.
(3) The *degree* $[E:F]$ of a field extension E of F.
(4) What it means for a number $\alpha \notin \mathbb{Q}$ to be *algebraic.*
(5) What it means for a field to be *algebraically closed.*
(6) The *Galois group* of a field extension, and of a polynomial.
(7) The *minimal polynomial* of a number $r \notin F$.
(8) What it means for an extension field E of F to be *normal.*
(9) What it means for group G to be *solvable.*
(10) A *ring* R.
(11) A *unit*, and a *zero divisor* of a ring.
(12) Types of rings: integral domain, division ring, principle ideal domain (PID), unique factorization domain (UFD), Euclidean domain.
(13) An *ideal* of a ring R (left, right, and two-sided).
(14) The *quotient ring* R/I for some two-sided ideal I, and how to multiply elements.
(15) A *homomorphism* ϕ from a ring R to a ring S.
(16) A *maximal ideal* M of a ring R.
(17) A *prime ideal* P of a ring R.

Useful facts and techniques.

(1) Use Eisenstein's criterion to show that a particular polynomial is irreducible.
(2) The degree of an extension $\mathbb{Q}(r)$ is the degree of the minimal polynomial of r.
(3) The Galois group of $f(x)$ acts on its n roots, and so $\mathrm{Gal}(f(x)) \leq S_n$. If f is irreducible, then this action has only one orbit.
(4) $|\,\mathrm{Gal}(f(x))| = [K:\mathbb{Q}]$, where K is the splitting field of $f(x)$.
(5) Know the statement of the Fundamental Theorem of Galois theory.
(6) Know the Galois groups of the following field extensions and be able to describe the explicit automorphisms: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)$, $\mathbb{Q}(\sqrt[4]{2},i)$, and $\mathbb{Q}(\zeta_n)$, where ζ_n is an n^{th} root of unity.
(7) Be able to construct the subfield lattices of the above fields, and demonstrate the Galois correspondence with subgroups of $\mathrm{Gal}(f(x))$.
(8) Know the Galois groups of the following polynomials: $f(x)=x^2-2$, $f(x)=(x^2-2)(x^2-3)$, $f(x)=x^3-2$, $f(x)=x^4-2$, $f(x)=x^n-1$.
(9) Summarize in a few sentences how to construct a degree-5 polynomial that is not solvable by radicals.
(10) Know examples of each of the following types of rings: integral domain, division ring, principle ideal domain (PID), unique factorization domain (UFD), Euclidean domain.
(11) Know examples of both maximal ideals and prime ideals.
(12) Learn how to construct a finite field $\mathbb{F}_q$ of order $q=p^k$.
(13) Know the statements of the fundamental homomorphism theorem and the correspondence theorem for rings and how to apply them.

Proofs to learn.

(1) Use Galois theory to prove that $\sqrt{2}$ is irrational.
(2) If an ideal I of R contains a unit, then $I=R$.
(3) The FHT for rings: if $\phi\colon R \to S$ is a ring homomorphism, then $\ker\phi$ is an ideal of R and $R/\ker\phi \cong \operatorname{im}\phi$.
(4) The following are equivalent: (i) I is a maximal ideal, (ii) R/I is simple, (iii) R/I is a field.
(5) An ideal P is prime iff R/P is an integral domain.

(6) A ring R is an integral domain iff 0 is a prime ideal.