Math 321 – Foundations of Abstract Algebra
Daily readings and examples

This document describes the short readings and examples you should bring to class each period. Page numbers refer to Gallian, and are generally just 1-2 pages. For your example, you should write it down and bring it to class and hand it in as you enter. Your example does not need a large write up, they should be able to fit on a half piece of paper. I am **not** asking you to write involved proofs for these.

Day	Reading	Example
Week 1		
Aug 29	31-34	Give an example of (1) two symmetries of a square which compose to give a reflection and (2) two symmetries of a square which compose to give a rotation.
Aug 31	42-43	Give an example of (1) A binary operation which is NOT associative (2) A binary operation which does NOT have an identity (3) A binary operation which has an identity but does NOT have inverses for every element
Sept 2	53	Give an example of (1) Two matrices A, B such that $AB = BA$ (2) Two matrices C, D such that $CD \neq DC$
Week 2		
Sept 5	60-61	Give an example of a finite group G and an element $g \in G$ such that g has order 13. Can you also do this with an infinite group G'?
Sept 7	41	Give an example of a subgroup of $(\mathbb{Z}, +)$. Give an example of an infinite subset of $(\mathbb{Z}, +)$ which is NOT a subgroup.
Sept 9	77-78 through #4	Give an example of an infinite group which is NOT cyclic.
Week 3		
Sept 12	93-94	Give an example of an infinite group which is not cyclic but has an infinite cyclic subgroup.
Sept 14	99-101	Give an example of a cycle in S_3 which has order 2. Give an example of a cycle in S_3 which has order 3.
Sept 16	114-115 Rubik's cube	Give an example of a group G so that the center of G is a proper, nontrivial subgroup of G.

Week 4

Sept 19	127-129	Give an example of an isomorphism from $\mathbb{Z}_6$ to itself. Give an example of a function from $\mathbb{Z}_6$ to itself which is invertible (1-to-1 and onto) but is NOT an isomorpihsm.
Sept 21	143	Give an example of two groups that appeared different to you at first, but turned out to be isomorphic.
Sept 23	144-145 (through Ex3)	Give an example of a group which is isomorphic to a proper subgroup of itself.

Week 5

Sept 26	161	Give an example of a non-inner automorphism of a group G.
Sept 28	162-163	Give an example of a finite group G, and a divisor d of $\|G\|$ such that G has no subgroup of order d. (Why does this not contradict Lagrange's theorem?)
Sept 30	154-156	Give an example of a finite group which is not isomorphic to a direct product of cyclic groups.

Week 6

Oct 3	185	Let H be the set of integer multiples of 5. What are the cosets of H in $\mathbb{Z}$?
Oct 5	169-172 cryptography example	I used the RSA algorithm (pg 171-172) with $p = 2557, q = 3391, e = 2843$ to encode a 2-letter message, with $A = 01, B = 02, \ldots, Z = 26$ as a 4-digit number M_1. I send you the number $R_1 = 4654114 = M_1^e \bmod pq$. What was the original message? (Feel free to use a calculator for finding things like $\mathrm{lcm}(p-1, q-1)$.)
Oct 7	Midterm 1	

Week 7

Oct 10	208-209	What familiar group is the quotient group $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$ isomorphic to?
Oct 12	225	Recall the center of $\mathrm{GL}_n(\mathbb{R})$ is the subgroup of diagonal scalar matrices (scalar multiples of the identity matrix). Describe the cosets of $Z(\mathrm{GL}_n(\mathbb{R}))$. Describe multiplication in the quotient group $\mathrm{GL}_n(\mathbb{R})/Z(\mathrm{GL}_n(\mathbb{R}))$. (This quotient group is called the **projective linear group**.)
Oct 14	45, 48-49	Give examples of group homomorphisms $\phi : G \to G'$ so that $\ker(\phi)$ is the trivial subgroup $\ker(\phi) = G$ $\ker(\phi)$ is a nontrivial, proper subgroup
Oct 17-21	Break	

Week 8

Oct 24	245-246	Describe two different ways that a ring can fail to be a group under multiplication.
Oct 26	246-248	Is the set $\{0\}$ a ring with the usual addition and multiplication? What about $\{0, 1\}$ with addition and multiplication mod 2?
Oct 28	255-256	(a) Give an example of a ring R and elements $a, b \in R$ with $a \neq 0, b \neq 0$ but $ab = 0$. (b) Give an example of a ring R' where property (a) cannot happen.

Week 9

Oct 31	207	(a) Give an example of a ring R and an element $a \in R$ with $a \neq 0$ but $a^3 = 0$. (b) Give an example of a ring R' where property (a) cannot happen.
Nov 2	267-268	Which of these statements is true? (a) Every ideal is a subgring. (b) Every subring is an ideal.
Nov 4	218-219	For any two groups G, H, there is the **trivial homomorphism** $\phi : G \to H, \phi(g) = e_H$ for all $g \in G$. Let G be a group with the property that for any group H, all homomorphisms $G \to H$ are trivial. In other words, there is exactly one group homomorphism $G \to H$ for any H. What can you conclude about G?

Week 10

Nov 7	287 Ex 9	Look up the *abc*-conjecture and just try to understand what it is saying, and how example 9 on page 287 is a special case of this. (No need to bring anything to class on paper.)
Nov 9	269	Let R be a ring and S a subring of R. What goes wrong if you try to construct a quotient ring as R/S? (i.e. why does S need to be an ideal for the quotient to be defined?)
Nov 11	271	If you replace the ideal $\langle x^2 + 1 \rangle$ in example 12 on page 271 with $\langle x^2 \rangle$, what is different? Describe the resulting quotient $\mathbb{R}[x]/\langle x^2 \rangle$. (This quotient ring is called the **dual numbers.**)

Week 11

Nov 14	298-300	What are the maximal ideals of $\mathbb{Z}$?
Nov 16	280	A ring is **Noetherian** if for any sequence of ideals $I_1, I_2, I_3 \ldots$ with $I_1 \subset I_2 \subset I_3 \subset \cdots$, there exists an n so that $I_n = I_{n+1} = I_{n+2} = \cdots$. In other words, every ascending chain of ideals "stabilizes." Is $\mathbb{Q}$ Noetherian? Is $\mathbb{Z}$ Noetherian?
Nov 18	320-322 Ex 12	Instead of 6-sided dice, suppose you have two 4-sided dice labelled 1,2,3,4. Is there another pair of 4-sided dice with other labels so that the probabilities are the same as with two standard 4-sided dice? (Only positive integers are allowed as labels.)

Week 12

Nov 21	Midterm 2	
Nov 23	260 Table 13.2	(a) Give an example of a non-commutative ring that has a unity and has characteristic 4. (b) Give an example of a commutative ring which has a unity, is not an integral domain, and has characteristic zero. (c) Give an example of an integral domain which is not a PID.
Nov 25	Break	

Week 13

Nov 28	311-313	Give an example of degree 3 polynomial which is reducible. Give an example of a degree 3 polynomial which is irreducible.
Nov 30	314-316	Give an example of a polynomial $f(x) \in \mathbb{Z}[x]$ which is irreducible as an element of $\mathbb{Z}[x]$, but becomes reducible when viewed in $\mathbb{Z}_2[x]$.
Dec 2	317-319	By Theorem 17.5, the polynomial $f(x) = x^5 - x^4 - 2x^3 - x^2 + x + 2$ has a unique factorization in $\mathbb{Z}[x]$. What is that factorization? (You can use a computer to help.)

Week 14

Dec 5	328-330	In each ring, describe the associates of an arbitrary element x. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}[x], \mathrm{M}_2(\mathbb{R})$
Dec 7	334-336	The ring $\mathbb{Z}[\sqrt{-3}]$ is not a unique factoriation domain. Give an example of an element in $\mathbb{Z}[\sqrt{-3}]$ with two distinct factorizations.
Dec 9	337-340	Give an example of a Euclidean domain which is not a principal ideal domain. Give an example of a principal ideal domain which is not a unique factorization domain.