ADVICE FOR STUDENTS FOR LEARNING ABSTRACT ALGEBRA

All references to specific exercises correspond to "Contemporary Abstract Algebra," 7th edition, Brooks Cole Cengage Learning, 2010 by Joseph A. Gallian

You should periodically reread this page as the course progresses since many of the comments refer to specific situations that will arise from time to time.

Unfortunately many students struggle with this subject. First and foremost you must study the material regularly. Don't wait until a day or two before an exam or when homework is due.

One of the greatest problems I see with students is that they do not have the definitions and the theorems memorized. They will come to my office and say that they can't do a certain problem such as prove some subset of a group is a subgroup. I will say to them "What does the One Step Subgroup Test say?" They won't know. Or I will ask them "What does $|a| = 6$ mean?" They will reply incorrectly that $a^6 = e$. Well, of course, if you do not know the definitions and theorems you won't be able to use them.

To learn to do proofs pick out several of the easier proofs that are given in the book (for instance, Example 5 of Chapter 3, Theorem 3.4 and Theorem 4.1). Write the statements down but not the proofs. Then see if you can prove them. Students often try to prove a statement without using the entire hypothesis. Keep in mind that you MUST use the hypothesis. If you cannot prove the statement, look at the first line of the proof in the text. That might be enough to get you started. If it is not, then look at the next line. Repeat this over and over until you can do them without looking at the text. Eventually you will get the hang of it. There is a direct relationship between your understanding of the subject and your ability to do proofs. Proofs test your understanding. They also test your creativity.

Keep in mind that you can only use what you have. For example, Exercise 12 in Chapter 3 says that if you have an Abelian (that is, commutative) group with two elements of order 2 then it has a subgroup of order 4. So we can let a and b be the two elements of order 2. Now all we have are a and b and the group axioms so USING ONLY a and b you must create a subgroup of order 4. Well, the axioms tell us that the identity is in the subgroup and closure tells us that ab is in there too so the subgroup must be $\{e, a, b, ab\}$. Then all we need do is to show that ab is distinct from the other three elements and use the Finite Subgroup Test to prove that this set is a subgroup.

Here is another example. Look at Exercise 60 on page 69. This exercise says to prove that every finite group with more than one element must have an element of prime order. Since the group has more than one element we may let a be a nonidentity element. If a has prime order we are done. If a does not have prime order then USING only a we must find an element of prime order. Since all we have to work with is a, the element of prime order has to be found using a. So, consider a, a^2, a^3, a^4 etc. One of these must have prime order. But how do we know which one? Well, try some abstract examples (not specific examples such as $U(n)$ or D_n) by supposing that $|a| = 15$. Then we see that $|a^3| = 5$. If we had $|a| = 12$, then $|a^4| = 3$. After trying several such examples we realize that if we write $|a| = pk$ where p is prime and $k > 1$ we have $|a^k| = p$. Note that we were able to do this problem using only the element a and closure.

Another thing that you must do is learn in **WORDS** what each concept given in symbols means. For example, $Z(G)$ is the set of all elements that commute with **EVERY** element of G while $C(a)$ is the set of all elements that commute with a. Likewise, you should think of $|a|$ as the **SMALLEST** positive power of a that gives the identity.

Whenever possible, convert words to symbols. For example, if you are given that a group G is finite write "Let $|G| = n$." If you are given that a group is Abelian write "We know that $ab = ba$ for all a and b." If you are asked to prove that a group is Abelian write "We want to show that $ab = ba$ for all a and b." If you are given that a group has an element has order 10. Write "We know that there is an element a such that $a^{10} = e$ and 10 is the least positive integer n such that $a^{10} = e$." If you are asked to prove that an element a has order 10 write "We want to show that $a^{10} = e$ and 10 is the least positive integer n such that $a^{10} = e$." If you are given that a group G is cyclic write "We know that there is an element g such that every element of G has the form g^n." If you are asked to prove that a group G is cyclic write "We want to find an element g such that every element of G has the form g^n." If you are given that x commutes with a write "We know that $xa = ax$." If you are asked to prove that x commutes with a write "We must show that $xa = ax$."

Use suggestive notation. For example, if a problem involves one element that is fixed and one that varies or is unknown, denote the fixed element by a and the variable element by x. For instance, since $C(a)$ is the set of all elements that commute with a, write "Let x belong to $C(a)$." If you are given two groups G and H denote the elements from G by g_1 and g_2 and the elements from H by h_1 and h_2 etc. Very often the statement of the problem suggests how to solve the problem. When you convert what you know from words to symbols and what you want to prove from words to symbols you often will be able to see how to proceed.

Whenever you are doing an exercise from the book or a problem on an exam you should ask yourself ``Is there a theorem in the book whose statement seems similar to the statement of the problem?" Most exercises and exams problems can be easily done by using one of the theorems in the book. For example, Exercise 17 of Chapter 2 asks to prove a group is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$. Notice that the latter condition appears similar to Theorem 2.4 (Socks-Shoes) and indeed using this theorem will provide a easy proof. Exercise 62 in Chapter 4 is a simply application of Theorem 4.2.

Here are some remarks about how to do algebra problems.

1. When you are asked to prove a statement you must not assume that the statement is true.

2. Never assume a group is Abelian. Some people begin their argument for Exercise 35 of Chapter 2 by saying "Assume that the group is Abelian." This is incorrect for you have no reason to assume a group is Abelian. Many groups are not Abelian.

3. Never divide group elements. Instead, use cancellation or inverses.

4. Never assume a group is finite when that condition was not stated.

5. In the text it is usually the case that elements of a group are denoted by letters from the beginning of the alphabet a,b, c or end of the alphabet x,y,z. Integers such as exponents and orders of elements or groups are usually denoted with letters from the middle of the alphabet i,j,k,m,n,s,t. For example, let $|a| = n$. You should use the same conventions.

6. When asked to find the inverse of an element, always check your answer by multiplying the element and its purported inverse to see if you get the identity. For example, to check that $(ab)^{-1} = b^{-1}a^{-1}$ all you need do is observe that $abb^{-1}a^{-1} = e$.

7. After you finish a proof look to see if you have used all the hypotheses. For example, if you were given that the group is Abelian check to see if

you used that condition in your argument. If the hypothesis says the group is finite check to see where you used finiteness. Occasionally, it may be the case that a given condition is not really needed but was there just to make the problem easier but usually all the given conditions are needed for the you to be able to give a valid proof with what you know at this point in the book.

8. Many exercises in the book involve a parameter n and ask you to prove something. (For example, Exercises 15, 19, and 20 in Chapter 2). You should look at the cases for small values of n such as 2 and 3 to gain insight and look for a pattern. This often tells you how to do the general case but keep in mind that doing specific values for n does not do the general case. The problem must be done for all n, not a few examples. In general, you cannot prove a statement is true by using specific examples.

9. When ask to provide an example to illustrate something, a dihedral group such as D_4 is often a good group to try. For example, Exercises 6 and 16 of Chapter 2.

10. On problems that ask for some answer rather that to prove something do not just give an answer. Show that your answer is valid. You must give reasons or an explanation of why your answer is correct. One example is "If $a_1,a_2,...,a_n$ belong to a group, what is the inverse of $a_1a_2...a_n$?" (Exercise 20 of Chapter 2). Give the answer and show that the product of $a_1a_2...a_n$ and your answer is the identity. Similarly, Exercise 14 of Chapter 4 asks "What is $|G|$?" Do not just give an integer. Give reasons why that answer is valid.

11. In many cases problems can be solved by simply writing out the expressions. For example in Exercise 26 of Chapter 2 write out $(ab)^2 = a^2 b^2$ as $abab = aabb$. Exercise 19 in Chapter 2 works the same way. Just write the expression out. (Many people incorrectly do Exercise 19 by using commutativity.)

12. Many theorems in the book about groups and elements of groups involve divisibility conditions and greatest common divisors of two integers. Divisibility only applies to integers. Infinity is not an integer. Do not talk about an integer dividing infinity or an integer being rel atively prime to infinity.

13. Whenever you say *"Assume ..."* you must have a reason why you may assume what it is you are assuming. For example, if you are given that H is a subgroup of G you may make the statement: Assume x is an element of H because subgroups are not empty. You cannot say "Assume G is

Abelian" without providing some reason why you may assume that G is Abelian. As another example, if you are given that a group is finite and a is an element of the group you may say "Assume $|a| = n$" because all elements of a finite group have finite order. However, if you do not know that the group is finite you can't assume that an arbitrary element from the group has finite order. Instead, you should take two cases. Case 1: $|a|$ is finite and Case 2: $|a|$ is infinite.

14. When doing a problem about the order of an element, such as proving that an element and its inverse have the same order, you will usually have to deal with the finite case and infinite case separately. That is, $|a| = n$ is one argument and $|a|$ is infinity is a different case. This is usually true as well when dealing with the order of a group. The cases of a finite group and an infinite group may require different arguments.

15. When asked for an example of something, use a specific example. For instance, in response to Exercise 6 of Chapter 2 some people say that matrices have the property that $a^{-1}ba$ is not equal to b. But you must actually give the specific matrices since some matrices have the desired property and some do not have the property.

16. In general, you cannot take roots (square roots, cube roots, etc.) in groups. Only integer powers of group elements are permissible.

17. Whenever you are asked to prove a subset of a group is a subgroup, use one of the subgroups tests. If you know the subset is finite use the Finite Subgroup Test. 18. When an exercise says prove something is true for an integer do not assume the integer is positive. In general, the cases that an integer is positive and an integer is negative require slightly different arguments. Usually, you can use the positive integer case to prove the negative integer case by using the Law of Exponents. To illustrate the technique consider Exercise 19 in Chapter 2. To prove $(a^{-1}ba)^n = a^{-1}b^na$ for all n , first prove it for positive n by writing out the expression $a^{-1}ba$ n times and canceling all the inner a and a^{-1} terms. (Alternatively, you could use induction.) To prove the statement when n is negative observe that $a^{-1}b^na = ((a^{-1}ba)^{-n})^{-1}$ and that $-n$ is positive. So, since you have already done the case when the exponent is positive you have $(a^{-1} ba)^n = ((a^{-1}ba)^{-n})^{-1} =$
$(a^{-1}b^{-n} a)^{-1}$. Then using the socks-shoes property you have $(a^{-1}b^{-n}a)^{-1} = a^{-1}b^na$. Finally, the case that $n = 0$ follows because any element to the 0th power is the identity by definition.

19. When dealing with an abstract group (that is, one in which the elements and operation are not specified) use e to denote the identity and

use multiplication as the operation (that is, ab). If you are told the operation is addition use $a + b$, $-a$ for the inverse of a, and 0 for the group identity.

20. The negation "for all" is "there exist some." For example, in an Abelian group $ab = ba$ for all a and b. So, in a non-Abelian group there exist SOME elements a and b such that ab is not ba. To remember this think of a common statement such as "The team won every game." The negation is "There exist some game the team did not win."

21. When ask to prove two groups are not isomorphic students often show that some specific mapping does not satisfy the definition of isomorphism. This merely proves that specific mapping is not an isomorphism. It does not preclude that some other mapping may be an isomorphism. Instead, one must show that NO mapping satisfies the definition. This can be done by assuming there is some generic isomorphism and using only properties of isomorphisms derive a contradiction. Examples 5 and 6 of Chapter 6 illustrate how this can be done. Notice that no specific mapping was assumed. Usually the easiest way to prove that two groups are not isomorphic is to show that they do not share some group property. For example, the group of nonzero complex numbers under multiplication has an element of order 4 (the square root of -1) but the group of nonzero real numbers do not have an element of order 4. As another example, we see that S_4 is not isomorphic to D_{12} because D_{12} has an element of order 12 whereas S_4 has elements of orders only 1, 2, 3 and 4. Often it is easiest to proceed by checking if the largest order of any element in each of the groups agree. When the orders of the elements in two groups match you can prove they are not isomorphic by showing that they have a different number of elements of some specific order. Exercise 35 of the Supplemental Exercises for Chapters 5-8 is such a case. When comparing the number of elements of some specific order, elements of order 2 is often a good choice.