

Required topics for Math 401—Modern Algebra, I

Updated:

11:30 Thursday 19th November, 2009

Grading.

The grading of the course will be based almost entirely on two tests and a final. The final will count as much as the two tests combined. Thus you will have to retain knowledge of the material to the end of the course.

There will be a small amount of homework collected and a few quizzes given. The combination of homework and quizzes will count no more than 10

There will be a certain amount of emphasis on “knowing what you are talking about.” Thus a few questions might check whether you know accurate definitions and statements of results.

Responsibilities.

This is to list what you will be responsible for. This list will change over time very rapidly. You should assume that several things will be added each week and that it is possible for it to change several times in as little as an hour. For an exam, you will be told which number range you will be responsible for. The contents of that range will not change from the time the exam is announced until the time of the exam.

The books are:

- (1) Bewersdorff’s *Galois theory for Beginners*, and
- (2) Allan Clark’s *Elements of Abstract Algebra*.

We will refer to the first as [B] and the second as [C].

- (1) You need to know that the formula for the solutions to a quadratic equation can be derived by completing the square and you have to know how to do the derivation.
- (2) You need to know how to argue that in solving polynomial equations, it suffices to look only at monic polynomials.
- (3) You need to know how to eliminate the second highest degree term from a polynomial equation.
- (4) You need to know how to find one root of a monic cubic equation with no second degree term.
- (5) You need to know how to do the arithmetic operations (+, −, ×, ÷) on complex numbers.
- (6) You need to know what a field is (all nine requirements), and that the rational numbers, the real numbers and the complex numbers each form a field.
- (7) You need to know how to find (using trig) the n -th roots of a complex number especially the special case consisting of the n -th roots of 1.
- (8) You need to know how to show that if S is a set of complex numbers with n different elements, and $z \neq 0$ is a complex number, then Sz has exactly n elements where Sz is the set of all wz with $w \in S$.
- (9) You need to know that the key fact in the previous item is the existence of the multiplicative inverse of z .
- (10) You need to know the basic algebraic properties of complex conjugation.

- (11) You need to know that if a polynomial has only real coefficients, then its non-real roots occur in complex conjugate pairs, you need to know that this fact follows from the algebraic properties of complex conjugation and you need to know how to make the argument.
- (12) You need to know the statement of the division algorithm for polynomials.
- (13) You need to know how to show from the division algorithm that if r is a root of $P(x)$, then $P(x)$ factors as $P(x) = (x - r)Q(x)$ for some polynomial $Q(x)$.
- (14) You need to know the statement of the Fundamental Theorem of Algebra.
- (15) You need to know what the natural numbers are, the integers, the rational numbers, the real numbers, and the complex numbers.
- (16) You need to know the statement of the well ordering property of the natural numbers.
- (17) You need to know how to use the well ordering property of the natural numbers to prove the division algorithm for polynomials.
- (18) You need to know how to express all the roots of a monic cubic polynomial equation (which has no quadratic term) in terms of one root of the equation (where the one root is found by the method learned in item (4) above).
- (19) You need to know the strategy for proving a statement with an “or” in the conclusion.
- (20) You need to know how to prove the following from the axioms of a field:
 - (a) For any x , $x + x = x$ implies $x = 0$.
 - (b) For any a , $a \cdot 0 = 0$.
 - (c) For any a and b , if $a \cdot b = 0$, then either $a = 0$ or $b = 0$.
- (21) You need to know that the distributive axiom is the key in proving the second item above.
- (22) You need to know the definition of a group.
- (23) You need to know the definition of an abelian group.
- (24) You need to know several examples of groups. For example:
 - (a) The complex n -th roots of 1 for a given natural n under multiplication.
 - (b) Any field under the addition of the field.
 - (c) The non-zero elements of any field under the multiplication of the field.
 - (d) The integers under $+$.
 - (e) The invertible $n \times n$ matrices with real entries under multiplication.
- (25) You need to know of each of your examples whether it is abelian or not.
- (26) You need to know why certain examples are not fields, such as integers under multiplication, complex n -th roots of 1 under addition and so forth.
- (27) You need to know what a subgroup is.
 - (a) You need to know that for any group G , one subgroup is the full group G .
 - (b) You need to know that for any group G , one subgroup is the set consisting of nothing but the identity.
- (28) You need to know what the order of an element of a group is.
- (29) You need to know how to prove that in a group there is only one identity and that each element of the group has only one inverse.
- (30) You need to know the definitions of the following:
 - (a) $f : X \rightarrow Y$ being a function.
 - (b) A function $f : X \rightarrow Y$ is onto.

- (c) A function $f : X \rightarrow Y$ is one-to-one.
 - (d) A function $f : X \rightarrow Y$ is a one-to-one correspondence.
 - (e) The composition $gf : X \rightarrow Z$ of the functions $f : X \rightarrow Y$ and $g : Y \rightarrow Z$.
- (31) You need to know how to prove the following:
- (a) If $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are both onto, then $gf : X \rightarrow Z$ is onto.
 - (b) If $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are both one-to-one, then $gf : X \rightarrow Z$ is one-to-one.
 - (c) If $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are both one-to-one correspondences, then $gf : X \rightarrow Z$ is a one-to-one correspondence.
- (32) If G is a group and S is a subgroup of G , then you need to know the definition of a right coset of S in G .
- (33) If G is a group, S is a subgroup of G , and Sx is a right coset of S in G , then you need to know how to show there is a one-to-one correspondence between S and Sx .

There will be a test on Thursday, October 1, 2009. It will cover items (1) through (33).

The next section will come primarily from Chapter 2 of [C]. Some preliminary work was done on permutations groups, permutations and conjugations. Thus some material was done out of order. However, we will go over Chapter 2 of [C] in order and will cover the preliminary material again. A few items to become familiar with from the preliminary material are as follows. An exercise will be included.

- (34) Know what the symmetric group $\mathcal{A}(X)$ on a set X is. The notation is that of §76 of [C], although that book does not use the phrase “symmetric group on X .”
- (35) Know what the symmetric group on n letters S_n is (§30 of [C]).
- (36) Know the Cauchy notation for an element of S_n (§78 of [C]).
- (37) Know the cycle notation of an element of S_n (the note after Theorem 80 of [C] and Theorem 80 itself).
- (38) Know how to get the order of an element of S_n from its cycle notation (the corollary to Theorem 80 of [C]).
- (39) Know how to multiply (compose) two elements of S_n if they are given in either Cauchy notation or cycle notation.
- (40) Know what the conjugation of x by y is and how to compute this with elements of S_n given either in Cauchy notation or cycle notation. (Conjugation is defined in §45 of [C], but what is defined there is conjugation of a subset by an element. To get what we want, replace the subset S by a set with a single element. The calculation of conjugation of elements of S_n is not laid out explicitly in [C]. However, it is implied that the student should have figured it out by the time exercise 80 α in [C] is done.)
- (41) Know how to find a conjugator that takes one permutation to another if they have the same cycle structure. This is based on a complete understanding of (40).

Exercise. Three groups will be given. For each make a table of conjugations. That is make a table that looks like a multiplication table but instead of putting xy in the position with x on the left and y above, put xyx^{-1} . That is, put the result of conjugating x by y .

In doing the calculations, you will use the information from (40). The second group is a group of permutations and you will be able to use the techniques for computing conjugates of permutations as referred to in (40). The first and third groups are not given as groups of permutations, and so you will need to just calculate from the definition of conjugation. If you like, you can turn each group into a group of permutations of its own elements as discussed in class (use left multiplication), but it is not clear that this will end up with a savings of effort. A sample calculation from the definition is given with the third group to make clear what is being asked.

The first group is the group of complex sixth roots of 1. These are

$$\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$$

where α has modulus 1 and argument $\pi/3$.

The second group is S_3 with elements (in cycle notation)

$$1 = (1)(2)(3)$$

$$a = (1\ 2)(3)$$

$$b = (1\ 3)(2)$$

$$c = (2\ 3)(1)$$

$$d = (1\ 2\ 3)$$

$$e = (1\ 3\ 2).$$

The third group is the group from Test 1 whose multiplication table is as follows:

	<i>M</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>
<i>M</i>	<i>S</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>M</i>
<i>I</i>	<i>P</i>	<i>M</i>	<i>K</i>	<i>Q</i>	<i>S</i>	<i>R</i>	<i>J</i>	<i>I</i>
<i>J</i>	<i>Q</i>	<i>R</i>	<i>M</i>	<i>I</i>	<i>K</i>	<i>S</i>	<i>P</i>	<i>J</i>
<i>K</i>	<i>R</i>	<i>J</i>	<i>P</i>	<i>M</i>	<i>Q</i>	<i>I</i>	<i>S</i>	<i>K</i>
<i>P</i>	<i>I</i>	<i>S</i>	<i>R</i>	<i>J</i>	<i>M</i>	<i>K</i>	<i>Q</i>	<i>P</i>
<i>Q</i>	<i>J</i>	<i>K</i>	<i>S</i>	<i>P</i>	<i>R</i>	<i>M</i>	<i>I</i>	<i>Q</i>
<i>R</i>	<i>K</i>	<i>Q</i>	<i>I</i>	<i>S</i>	<i>J</i>	<i>P</i>	<i>M</i>	<i>R</i>
<i>S</i>	<i>M</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>

To be clear about this exercise, we mention that entry in the multiplication table above in the row with J at the left and where K is at the top has I since $JK = I$. In the exercise, this should be replaced by the conjugate of J by K or $KJK^{-1} = KJR$ since the fact that $KR = S$ and S is the identity of the group implies that $K^{-1} = R$. Thus the entry in the table being constructed with J at the left and K at the top will have $KJR = PR = Q$.

Chapter 2 of [C].

In what follows, Chapter 2 of [C] will be described in order with various parts identified as parts to be read, parts to be skipped, and exercises to be done. You will not be asked questions about parts to be skipped. “Read” means read and learn the content.

The list that follows will run well ahead of what we will do in class. You will be told how far down the list to go each day.

- (42) Read: The introduction to Chapter 2 (P. 17).
- (43) Read: §26 (P. 17–18).
- (44) Skip: §§26 α –26 ϵ (P. 18). These come under the heading of “fun with the axioms.”
- (45) Read: §26 ζ (P. 18).
- (46) Read: §26 η (P. 18).
- (47) Exercise: §26 θ (P. 19).
- (48) Read: §26 ι (P. 19).
- (49) Skip: §§26 κ –26 ν (P. 19).
- (50) Read: §27 (P. 19–20).
- (51) Skip: §§27 α –27 γ (P. 20).
- (52) Read: §28 (P. 20) and learn the proof.

- (53) Exercise: §28 α (P. 20).
- (54) Exercise: §28 β (P. 21). You already know how to do this.
- (55) Exercise: §28 γ (P. 21). This is a very important example of “fun with the axioms.”
- (56) Skip: §28 δ (P. 21).
- (57) Read: §29 (P. 21).
- (58) Exercise: §29 α (P. 21).
- (59) Skip: §29 β (P. 21).
- (60) Exercise: §29 γ (P. 21).
- (61) Skip: §29 δ (P. 21). This was done in class as an example of “fun with the axioms.” It is a nice result, but we will never use it.
- (62) Read: §30 (P. 22).
- (63) Exercises: §§30 α –30 γ (P. 22).
- (64) Read: §31–32 (P. 22).
- (65) Read: §17 (P. 9). This topic will be discussed in detail in class. When this and pages 10 and 11 are finished, we will resume with Chapter 2.
- (66) Know the definitions of “reflexive,” “symmetric,” and “transitive.” These three words are, respectively, (a), (b), (c) in the definition of *equivalence relation* in §17, Page 9 of [C]. The three words are not used in the book. Know the definition of an equivalence relation. §17 (P. 9).
- (67) Know the definition of *subgroup* of a group. §35 (P. 24).
- (68) Let G be a group and let H be a subgroup of G . Know the definition of a *right coset* of G in H . The book does this very badly. The sets Hy in §37 β are the right cosets of H in G , and the book never directly admits that this is the definition. The “definition” is given for left cosets in §37, and the definition used there is much more complicated than necessary. However, the book’s definition is justified if you do (a) in the next item.
- (69) Let G be a group and H a subgroup of G . Let x and y be elements of G .
- (a) Know how to prove that defining $x \sim_H y$ as “there is a right coset of H in G that contains both x and y ” is equivalent to defining $x \sim_H y$ as “ xy^{-1} is an element of H .”
- (b) Know how to prove that \sim_H is an equivalence relation.
- This is the “reverse” of what is done in §37 (P. 26). The relation there is based on $x^{-1}y$ rather than xy^{-1} and the result is that the book is looking at left cosets rather than right cosets. Other than minor differences arising from this reversal, the logic is the same. However, you cannot copy what is there word for word. You will have to think or consult your notes.
- (70) Let S be a set, let \sim be an equivalence relation on S , and let $x \in S$. Know the definition of $[x]$, the equivalence class of x under \sim . (In §17, Page 9 with slightly different notation.)
- (71) Let S be a set and let \sim be an equivalence relation on S . Let x and y be elements of S . Know how to prove that either $[x]$ and $[y]$ are identical or disjoint. (This is mentioned but not proven in §17, Page 9. You will need your notes.)
- (72) Let S be a set and let \sim be an equivalence relation on S . Know what “the well definedness problem” is for an operation defined on the equivalence classes of \sim . This is not defined in the book. An example of a “solved” well definedness problem is §18 α (P. 10). The sentence in parentheses at

the end of that item is an announcement that the well definedness problem has been solved without any explanation.

- (73) Let G be a group and let H be a subgroup of G . Know the definition of “ H is normal in G .” The definition in the book does not come until §46 (P. 32) and is the standard definition. The definition we give is much simpler and has fewer words that need to be digested. Later we will prove that our definition is equivalent to the one in the book. Consult your notes for our definition.
- (74) Know why every subgroup in an abelian group is normal. I cannot find a direct mention of this in [C].
- (75) Let G be a group and let H be a subgroup of G . Define \sim_H as in (69). Know how to show that the multiplication on equivalence classes defined by $[x][y] = [xy]$ is well defined when H is a normal subgroup of G . This is done in §47 (P. 34) where they use “left” while we use “right.” This is similar to the relationship between our (69) and §37 in [C]. However, the argument in the book is very different beyond the switch from left to right. We will discuss the difference when we get there. Rely on your notes.
- (76) Read: §33 (P. 23). This is a resumption of our march through Chapter 2. The point here is that \mathbf{Z} is abelian and that $n\mathbf{Z}$, the set of all multiples of n in \mathbf{Z} is not only a subgroup, but a normal subgroup. The book seems to have forgotten that the well definedness problem they raise was previously done in §18 α .
- (77) Skip: §34 (P. 23). We may revive this *much* later in the course.
- (78) Read: §35 and §35 α (P. 24). These go together because of the proposition in §35. The proposition is odd. It has a hypothesis (the finiteness of H) that is used but its importance is never explained. Because H might be infinite, you also need to know §35 which works whether H is finite or infinite. Because of this “gap” in the book’s flow of ideas, we will fill it in with the next item.
- (79) Know an example where the proposition in §35 fails. Obviously, H will have to be infinite. Consult your notes.

There will be a test on Thursday, November 5, 2009. It will cover items (34) through (79).

- (80) Read: §35 β (P. 24). This kind of argument occurs repeatedly in many mathematical subjects.
- (81) Exercise: §35 γ, δ . There are really three exercises here since there are three things that have to be shown are subgroups.
- (82) Read: §35 ϵ . This can be rather subtle. There are several things to show. First that a smallest subgroup exists with the required properties. Second, one shows that this subgroup contains a specific set of elements. The second argument is an equality of two sets and one needs to show two containments.
- (83) Exercise: §35 ζ (P. 25). The last part can involve a lot of work. It is easiest to attack by noting that two elements commute if and only if the conjugate of one (call it x) by the other (call it y) is x . Then recall that xyx^{-1} moves things exactly as x does except the movement is shifted by y . Thus if x fixes a vertex v , then xyx^{-1} fixes $y(v)$ and so forth. It is then very easy to show that there are a lot of pairs that do not commute. Compute xyx^{-1}

this way for y a power of α and x one of the $\alpha^i\beta$. It will then become clear what pairs commute. The “where things move” view of conjugation is extremely important.

- (84) Exercise: §35 η (P. 26).
- (85) Skip: §35 θ (P. 26). If this turns out to be important, we will come back to it.
- (86) Skip: §36 and §36 α – δ (P. 26). This is a nice topic, and we might get back to it later. However, we want to get to other things first.
- (87) Read: §37 §37 α, β (P. 26–27). We have discussed this in detail, but with right cosets instead of left cosets. This can be reviewed with your notes on the right cosets in hand to see where the (very minor) differences are. Note left cosets are defined in §37 and right cosets are defined in §37 β .
- (88) Exercise: §37 γ (P. 27). This is trivial but do it anyway. It involves proving equalities of sets.
- (89) Exercise: §37 δ (P. 27). This is of extreme importance. We add to the exercise. Let H be a subgroup of S_n . Define a relation \sim on H by $\pi \sim \tau$ if $\pi n = \tau n$. This looks just like the relation that the exercise defines on S_n . The only difference is that we only look at elements of H . Prove that this is an equivalence relation. (The book does not ask you to do that for S_n because it is a trivial exercise, but do it anyway.) Show that this equivalence relation is congruence modulo a subgroup of H . THEN define $H(n) = \{\pi n \mid \pi \in H\}$. This is the set of all places that H takes n and is called the *orbit* of n under H . Prove that there is a one-to-one correspondence between $H(n)$ and the set of equivalence classes under \sim in H .
- (90) Read: §38 (P. 27).
- (91) Exercise: §38 α (P. 27). This is a big problem. The first thing to do (second sentence of the problem) is not hard if done carefully. The second thing to do (third sentence of the problem) is harder. The set HK is a union of right cosets of H . (It is also a union of left cosets of K , but we don't have to work with both points of view.) However, if we look at all Hk as k runs over K , we do not get that all the right cosets of H that we get are different. The problem is to decide when two different cosets Hk_1 and Hk_2 are the same for different elements k_1 and k_2 of K . Then decide how much difference this makes in the calculation of $o(HK)$.
- (92) Skip: §38 β (P. 27).
- (93) Exercise: §38 γ (P. 28). Hint: Take some non-identity element x of G and look at $\langle x \rangle$. What must be true? Now what must be true if $o(G)$ is not prime?
- (94) Exercise: §38 δ (P. 28). The method of proof of this exercise has absolutely nothing whatever to do with the topics surrounding the problem. However, the method is based entirely on counting. Its conclusion does fit with the surrounding topics. If there is a non-identity element a whose square is the identity, then $\langle a \rangle$ is a subgroup with two elements. So this problem says that every group of even order has a subgroup of order 2.
- (95) Read: §39 (P. 28). In the proposition the words “it is easy to see that” appear. These words need translation. They mean “once you have done the work to see it the first time, or once you have been shown it by someone

else, then it is easy to see it from that time forward.” The proposition follows trivially from Lagrange’s Theorem (§40).

- (96) Exercise: §39 α (P. 28). Just count everything.
- (97) Exercise: §39 β (P. 28). The interesting part of the exercise is the symbol \leq . What is the difference between the situation where $<$ is true and the situation where $=$ is true.
- (98) Read: §40 (P. 28–29). This is hugely important and has already been discussed.
- (99) Read: §41 (P. 29). This has already been discussed.
- (100) Exercise: §41 α (P. 29).
- (101) Exercise: §41 β (P. 29). The important word here is “abelian.” Find an example in a non-abelian group where things go wrong.
- (102) Exercise: §41 γ (P. 29). This has been done. The book is looking for the “algebraic” proof, and not the permutation proof.
- (103) Exercise: §41 δ (P. 29). In spite of the fact that things go wrong in non-abelian groups, what goes wrong for ab is no different from what goes wrong with ba . The proof uses a fact that is too important to leave buried in a problem. Show the following fact: ab and ba are conjugate.