SYLLABUS

MA 312 ABSTRACT ALGEBRA WITH APPLICATIONS

Don Faust
Department of Mathematics and Computer Science
Northern Michigan University

MA 312
3 credit hours
Prerequisites: MA 211 and MA 163, or instructor's permission
Bulletin Description: Topics chosen from universal algebraic notions, graphs, trees, lattices, Boolean algebras, groups, rings, fields, and applications

FOUR FOUNDATIONAL REFLECTIONS CONCERNING THE COURSE

1. Mathematics as Approximative Modeling

As one grows mathematically, one sees more clearly that part of the work of doing mathematics is constructing *approximative models* of the Real World (hereafter R). Here I am thinking of R as

> not only the physical world (or, more precisely, our ever-expanding partial and tentative <u>knowledge</u> of the physical world) investigated by such sciences as physics, chemistry, and biology

but also as

> those many other parts of 'our world' (more precisely, again, our … <u>knowledge</u> of it) investigated by such sciences as psychology, sociology, and economics.

While paying due homage to the intrinsic beauty of mathematics, it is just as true that mathematics is a <u>service industry</u>: we build modeling tools for science, and indeed for any enterprise which wishes to pursue its goals with as much rationality, rigor, and depth as can be mustered. In fact, we not only *build* these tools, we *analyze* the tools both deductively (studying what is logically entailed within the tool) and semantically (studying the variety of models encompassed by the tool), helping our fellow scientists

both in generating better understanding of the tool and in finding refinements of the tool – leading of course to the 'next generation' of ever-improving tools.

Our Abstract Algebra course is an excellent one to further deepen one's understanding of this nature of mathematics. As the course unfolds, I anticipate that you will see many reasons for this. But let me briefly list three of them here, and then say a word about each: the students are 'ready', the content is superbly appropriate, and the methodology is 'hands on'. Firstly, students tend to come to the Abstract Algebra course with some mathematical maturity in hand, for example having already taken Elementary Calculus and Linear Algebra, and hence this prior exposure to a variety of mathematical structures can form a foundation upon which a successful growth experience in Abstract Algebra can be built. Secondly, the classes of models normally dealt with in Abstract Algebra – groups, rings, fields, vectors spaces and so on – have a crispness, a simplicity, and a connection to prior mathematics experiences of the students, which makes Abstract Algebra an excellent medium for the achievement of a deepening of understanding toward which we hope to help the students move. Finally, unlike the undergraduate courses in mathematical logic and in the history of mathematical thought where the former is often presented abstractly and foundationally while the latter is often presented as a survey so that neither course has the time to look at mathematical particulars in sufficient depth, in Abstract Algebra we focus on a few carefully chosen classes of models and really dig in and get our hands dirty - providing real experiences of grappling with these classes, experiences upon which the greater depth of understanding we seek can be based.

2. Remarks Concerning the Foundational Framework

In this course one of our ambitions is to uncover, and become scientifically comfortable with, the above work of doing mathematics. Depending on the area of R being investigated, appropriate languages are constructed, involving relevant predicate and function symbols. Then the syntax (and *'proof' machinery*) of the language at hand is carefully delineated. Further, an appropriate semantics (and *'truth' machinery*) for the language is also delineated, involving a 'model space' of appropriate <u>structures</u>: each <u>structure</u>, or <u>model</u>, $\mathbb{A}$ provides a non-empty set A of objects of the structure (the 'universe' of the structure) together with an appropriate interpretation for each of the predicate and function symbols in the language. Namely, for each n-ary predicate symbol P in the language, its interpretation in $\mathbb{A}$, denoted $P^{\mathbb{A}}$, is an n-ary relation on A (a subset of A^n); and for each n-ary function symbol F in the language, its interpretation in $\mathbb{A}$, denoted $F^{\mathbb{A}}$, is an n-ary function on A (a mapping from A^n to A).

It is possibly most important that we study the ***structure-preserving mappings*** between these models: they are called *homomorphisms*, and we will be particularly interested in them. Let $\mathbb{A} = \langle A,\ldots\rangle$ and $\mathbb{B} = \langle B,\ldots\rangle$ be structures in a language L

(the ellipses in A and in B, if elaborated, would provide the interpretations, as explained above, of the predicate and function symbols of L in A and B respectively), and let

$$g: A \rightarrow B$$

be a function from the universe of A to the universe of B. Then we say that g is a <u>homomorphism</u> from A to B iff

(1) for each n-ary predicate symbol P of L and each n-tuple $<a_1,\ldots,a_n>$ in A^n,

$$\text{if } <a_1,\ldots,a_n> \text{ is in } P^A, \text{ then } <g(a_1),\ldots,g(a_n)> \text{ is in } P^B,$$

and

(2) for each n-ary function symbol F of L and each n-tuple $<a_1,\ldots,a_n>$ in A^n,

$$g\,(\,F^A\,(<a_1,\ldots,a_n>)\,) \;=\; F^B\,(<g(a_1),\ldots,g(a_n)>).$$

Actually, any n-ary function symbol can be *rendered* as an (n+1)-ary predicate symbol with two simple FDs (FD = 'Framework Delineator', as explained in class) and an encoding assertion, so let's take a moment to see how that is done. Let F be an n-ary function symbol. We *render* F as the (n+1)-ary predicate symbol P_F as follows. We first assert that the (n+1)-ary predicate symbol P_F is *n-ary functional* with the following two FDs:

(a) for all $v_1,\ldots,v_n$ there exists y such that $P_F\,(v_1,\ldots v_n,y)$, and
(b) for all $v_1,\ldots,v_n,y_1,y_2$ $(\,(\,P_F\,(v_1,\ldots v_n,y_1)$ AND $P_F\,(v_1,\ldots v_n,y_2)\,) \rightarrow y_1 = y_2)$.

Then one asserts that P_F *encodes* F as follows:

(c) for all $v_1,\ldots,v_n,y$ $(\,F\,(v_1,\ldots,v_n) = y$ IFF $P_F\,(v_1,\ldots,v_n,y)\,)$.

Let us further note, in the context of the mapping g above, that the equation in (2) *is equivalent to* the assertion (*) that for each (n+1)-tuple $<a_1,\ldots,a_n,a>$ in A^{n+1}

$$\text{if } <a_1,\ldots,a_n,a> \text{ is in } P_F{}^A, \text{ then } <g(a_1),\ldots,g(a_n), g(a)> \text{ is in } P_F{}^B. \qquad (*)$$

A proof of this equivalence goes as follows. Indeed, it's nice (don't YOU think so too?) if our syllabus for MA 312 Abstract Algebra contains at least one theorem and its proof, so let's state and prove our equivalence as such!

THEOREM.

In the context of the mapping g above, the equation in (2) above holds iff assertion (*) holds.

PROOF.

$\rightarrow$:
To show that (2) implies the above assertion (*), assume (2), that $<a_1,\ldots,a_n,a>$ is in A^{n+1}, and that $<a_1,\ldots,a_n,a>$ is in $P_F^{\mathbb{A}}$. Then by the fact that P_F renders F (i.e. P_F is the relational coding of F described above), $a = F^{\mathbb{A}}(<a_1,\ldots,a_n>)$, so by (2) $g(a) = F^{\mathbb{B}}(<g(a_1),\ldots,g(a_n)>)$ and hence (again since P_F renders F) $<g(a_1),\ldots,g(a_n), g(a)>$ is in $P_F^{\mathbb{B}}$.

$\leftarrow$:
Now let us show that, conversely, the above assertion (*) implies (2). Assuming the above assertion (*) and that $<a_1,\ldots,a_n>$ is in A^n, since P_F renders F and hence

$$< a_1,\ldots,a_n, F^{\mathbb{A}}(<a_1,\ldots,a_n>) > \text{ is in } P_F^{\mathbb{A}},$$

we infer from the above assertion (*) that

$$<g(a_1),\ldots,g(a_n), g(F^{\mathbb{A}}(<a_1,\ldots,a_n>)) > \text{ is in } P_F^{\mathbb{B}};$$

but, also, again since P_F renders F, we infer that

$$<g(a_1),\ldots,g(a_n),F^{\mathbb{B}}(< g(a_1),\ldots,g(a_n)>)> \text{ is in } P_F^{\mathbb{B}},$$

so since P_F is n-ary functional (so the final coordinates in the above two (n+1)-tuples must be the same, by condition (b) in the definition above describing the n-ary functionality of P_F, since these two (n+1)-tuples agree in their first n coordinates) we conclude that

$$g(F^{\mathbb{A}}(<a_1,\ldots,a_n>)) = F^{\mathbb{B}}(< g(a_1),\ldots,g(a_n)>).$$ // **(end of the proof)**

Hence, if each function symbol F were to be replaced by its relational rendering P_F as delineated above, then for the resulting entirely relational language condition (1) would be sufficient to capture the assertion that g is a homomorphism from $\mathbb{A}$ to $\mathbb{B}$, and condition (2) could be dispensed with.

Thinking carefully about this, as the semester unfolds, may help in deepening one's understanding of the nature of structure-preserving mappings. For example, one of the major classes we will consider this semester will be *groups*. The language L_{groups} of groups will contain a binary function symbol * (to be used for the group's binary operation), a unary function symbol -1 (to be used for the group's unary 'inverse' operation), and a 0-ary function symbol e (to be used for the group's 0-ary 'identity' operation (constant)). It may help later, when we are considering homomorphisms from one group to another, to consider the associated relational language as discussed above, containing respectively a ternary relation symbol P_*, a binary relation symbol P_{-1}, and a unary relation symbol P_e, each made functional via appropriate versions of (a) and (b) above and each made to encode the associated function symbol via an appropriate version of (c) above.

This example is so central to our work in this course that it deserves a careful look. So suppose $\mathtt{G} = < G, *^{G}, -1^{G}, e^{G} >$ and $\mathtt{H} = < H, *^{H}, -1^{H}, e^{H} >$ are structures in the language L_{groups} as described above, and that g is a function from the universe of $\mathtt{G}$ to the universe of $\mathtt{H}$:

$$g: \ G \rightarrow H.$$

(It is important to note here that it is not necessary that $\mathtt{G}$ and $\mathtt{H}$ actually be groups, i.e. that they satisfy a set of FDs for 'Group Theory' (see e.g. page 25 of our text). It is particularly important to note this since I have chosen to use the usual Group Theory names for the operations involved, keeping in mind that in our course part of our focus will be Group Theory. In other words, to define the notion that g is a homomorphism it is sufficient that $\mathtt{G}$ and $\mathtt{H}$ are structures associated with the language L_{groups} at hand.)

By definition, then, g is a homomorphism from $\mathtt{G}$ to $\mathtt{H}$ just in case, instantiating (2) for the function symbols *, -1, and e of the present example of L_{groups}, the following hold:

for the binary function symbol * of L_{groups} and each ordered pair $<a_1,a_2>$ in G^2,

$$g\ (\ *^{G}\ (<a_1,a_2>)\ )\ =\ *^{H}\ (<g(a_1),g(a_2)>)$$

which is, in the more common infix notation of Abstract Algebra for binary operations,

$$g\ (a_1\ *^{G}\ a_2)\ =\ g(a_1)\ *^{H}\ g(a_2);$$

for the unary function symbol -1 of L_{groups} and each a in G,

$$g\ (\ -1^{G}\ (a)\ )\ =\ -1^{H}\ (g(a))$$

which is, in the more common superscripted postfix notation of Abstract Algebra for inverse operations,

$$g\ (\ a^{-1_G}\ )\ =\ g(a)^{-1_H};$$

and for the 0-ary function symbol e of L_{groups}, where since $G^0 = H^0 = 1 = \{\phi\}$,

$$g\ (e^{G}(\phi))\ =\ e^{H}(\phi)$$

which is, in the more common notation of Abstract Algebra for constants,

$$g\ (e^{G})\ =\ e^{H}.$$

Finally, let us provide these three homomorphism conditions in the context of the entirely relational language associated with L_{groups}, according to the appropriate instantiation of (1):

for the ternary predicate symbol P_* (rendering the binary function symbol *) and each ordered triple $<a_1,a_2,a_3>$ in G^3,

$$\text{if } <a_1,a_2,a_3> \text{ is in } P_*^{G}, \text{ then } <g(a_1),g(a_2),g(a_3)> \text{ is in } P_*^{H}$$

(that is, this condition asserts that for $<a_1,a_2,*^{G}(<a_1,a_2>)>$ in P_*^{G}, $<g(a_1),g(a_2),g(*^{G}(<a_1,a_2>))>$ is in P_*^{H}) ;

for the binary predicate symbol P_{-1} (rendering the unary function symbol -1) and each ordered pair $<a_1,a_2>$ in G^2,

$$\text{if } <a_1,a_2> \text{ is in } P_{-1}^{G}, \text{ then } <g(a_1),g(a_2)> \text{ is in } P_{-1}^{H}$$

(that is, this condition asserts that for $<a_1,-1^{G}(a_1)>$ in P_{-1}^{G}, $<g(a_1),g(-1^{G}(a_1))>$ is in P_{-1}^{H}) ;

and for the unary predicate symbol P_e (rendering the 0-ary function symbol e) and each a in G,

$$\text{if a in } P_e^{G}, \text{ then g(a) is in } P_e^{H}$$

(that is, noting here that $P_e^{G} = \{e^{G}(\phi)\} =_{\text{notation}} \{e^{G}\}$ and $P_e^{H} = \{e^{H}(\phi)\} =_{\text{notation}} \{e^{H}\}$, this condition simply asserts that $g(e^{G}) = e^{H}$) .

3. Two Fundamental Results Concerning the Foundational Framework

There is of course a considerable foundational framework underpinning the mathematical work of which we are speaking here. Possibly the most important element of this framework, indeed relevant to our work in all of the deductive sciences, is the Deduction Theorem for First-Order Logic. Here it is. Let Σ be a set of sentences and let α and β be sentences.

THEOREM (Deduction Theorem, Herbrand 1930).

If there is a proof of β from Σ UNION $\{\alpha\}$, **then** there is a proof of $\alpha \rightarrow \beta$ from Σ.

This theorem justifies our routine *modus operandi* in the deductive sciences, of proving an implication $A \rightarrow B$ by deducing B from an assumption of A. Note, incidentally, that the converse of this theorem follows trivially by a single application of the rule of inference *modus ponens*.

Also of great importance for our mathematical work is Goedel's Completeness Theorem for First-Order Logic. Arguably the most important theorem of 20th century logic, it was Goedel's doctoral dissertation under Hans Hahn at the University of Vienna. (It was followed the next year by Goedel's Incompleteness Theorems, very interesting and important impredicative results: but those must remain a story for another day.) It runs as follows. Let Σ be a set of sentences and let α be a sentence.

THEOREM (Completeness Theorem, Goedel 1930).

If every model of Σ is a model of α, **then** there is a proof of α from Σ.

This theorem informs us regarding our having set things up well, in fact asserting that our proof theory is 'strong enough': if a sentence α is true in every model of Σ, then there is a proof of α from Σ.

Let us also note that the converse of this result holds too: it is easier to prove, was proven earlier, and is called the Soundness Theorem for First-Order Logic. It also informs us regarding our having set things up well, asserting that our proof theory is 'not too strong': if there is a proof of a sentence α from Σ, then α is true in every model of Σ (i.e. there is no model of Σ in which α is false).

4. Remark Concerning the Specific Course Content

The question of how to further initiate students into this deeper, more comprehensive, view of the nature of mathematics, *that mathematics is in the very interesting (and useful!) business of providing a rich and constantly evolving toolbox of machinery and techniques for the construction and use of approximative models of* R, is of course a very interesting one. Currently, based on the considerable thought and experience of the mathematics community in regard to this question, the general tendency is to proceed as follows: we select a small collection of classes of such approximative models, each class being rich in structure and exemplary in its broad range of applications, and study this collection carefully. Examples of commonly selected classes are groups, rings, fields, and vector spaces, and in our course most of these classes will likely be in the collection we will choose to study carefully.

Indeed, in the text for our course (by Pinter, cf. below), we will tentatively study
groups in Chapters 1-16,
rings, integral domains, and fields in Chapters 17-20, and
vector spaces in Chapter 28.

Welcome aboard! Have a great and growthful ride! And, let me close this overview with the following remark:

> our course can be a very exciting journey (if your involvement is sincere and includes both good class attendance and a parallel daily commitment to hammering things out on your own through daily study and problem-solving), at the end of which you will find not only that your mathematical maturity has been substantially enriched, but also that the general analytical skills you bring to bear in the broader arena of your daily life in the Global Village will be substantially enriched as well.

DETAILS CONCERNING THE COURSE

Text:

A Book of Abstract Algebra by Charles Pinter

Evaluation:

Firstly, in addition to ungraded daily assignments, there will be a sequence of graded SUBMITTED ASSIGNMENTS (SAs) which can be resubmitted repeatedly until satisfactory. And there will probably be a DIARY kept and at least one CLASS PRESENTATION.

Secondly, there will be three mid-semester exams and a final exam. Only very exceptional circumstances could justify missing an exam; in these rare cases, permission must be requested in advance, and a make-up exam (usually oral) will occur later in the semester.

The evaluation framework is as follows (please note especially the dates, already fixed, when the three mid-semester exams will take place):

Exam 1:	Wed	26 Sept	150 points
Exam 2:	Wed	24 Oct	150 points
Exam 3:	Wed	28 Nov	150 points
Final Exam:			350 points
Diary / Class Presentation(s):			50 points
Submitted Assignments (SAs): to be submitted en masse by Friday 30 Nov for grade recording			150 points
		Total:	1000 points

Grading:

90-100%, A; 80-89%, B; 70-79%, C; 60-69%, D; 0-59%, F. The grading may be less stringent, but not more stringent, than this.

Note regarding special needs:

If you have a need for any disability-related accommodations or services, please inform the Coordinator of Disability Services Office in 1104 University Center (227-1737). Reasonable and effective accommodations and services will be provided to students if requests are made in a timely manner, with appropriate documentation, in accordance with federal, state, and university guidelines.

FRAMEWORK DELINEATORS (FDs)

Though we sometimes speak of the 'axioms' or 'assumptions' which occur in our building of the syntactic and semantic frameworks of the *approximative modeling* work we do in mathematics, if we are being careful and precise as scientists then we surely note that there is no need, in terms of what we do when we do science, for any assertion that these 'axioms' or 'assumptions' are True in the Real World (R).

Indeed, each time we are involved in this work of 'doing mathematics', we are simply constructing *frameworks*, analyzing our collected data

[**either** theorems provable within the framework **or** empirical information related to the framework],

and assessing the approximativity of our model.

From the perspective of ***explorationism*** (see my short paper

"Conflict without Contradiction: Noncontradiction as a Scientific Modus Operandi", PROCEEDINGS OF THE 20TH WORLD CONGRESS OF PHILOSOPHY, at www.bu.edu/wcp/Papers/Logi/LogiFaus.htm, 1999, five pages

which explicates this perspective concerning the nature of science), in science we are roughly involved iteratively in the following 4-step loop of investigating the utility of our approximative modeling in furthering our still often meager understanding of R:

(1) we construct **Framework Delineators (**FDs**)** in building our approximative model, then

(2) on the basis of *commitment* (no belief in the Truth of these FDs is needed) we implement entailed actions (e.g. proving theorems, conducting experiments), then

(3) we study the consequences of these actions, and finally

(4) we adjust our FDs according to what we have learned from our actions and their consequences, and finally we loop back to (2) to learn more.

Nowhere in this process of 'doing science', we suggest, is any belief needed.

Indeed, in doing our work in the iteration of the loop given above, we are simply iteratively analyzing our collected data, assessing the approximativity of our model, and adjusting the model.

Because of this, let us hereafter refrain from the use of such labels as 'axioms' or 'assumptions': let us instead refer to these sentences, which are really just part of our 'laying out' of the framework of the approximative model we are building, as **Framework Delineators (**FDs**)**.

SUBMITTED ASSIGNMENTS (SAs)

Whether or not the question asks for it, in each problem give a nice written commentary about what you are doing AND in each problem where it is appropriate include graphs *or other visualizations* which help in seeing what is going on.

Always state the problem clearly. If it involves you in a proof of any kind, be very clear about what you are proving and about each step you take in the proof.

Hand them in as you do them, repeatedly if needed.

If I put a check at the top, it's done; if I don't, it isn't.

Always put the SA #, together with the problem designation (e.g. "SA # 1: problem 3.A.2"), at the top of the sheet you hand in.

Do each carefully, as a nice piece of mathematics!

You must submit them ALL TOGETHER before or on the final due date (*see your syllabus for the date*) in order for your grade on your SAs to be recorded!

Your 15 submitted assignments (SAs), 10 points each for 150 points total for the semester, are as follows:

SA number	PROBLEM(S) INVOLVED	TOPIC (roughly)
SA # 1	**3.A.2**	**groups**
SA # 2	**4.C.1-7**	**properties of groups**
SA # 3	**5.B.4 & 5.D.3**	**subgroups**
SA # 4	**14.C.3**	**group homomorphisms**
SA # 5	**14.C.4**	**group homomorphisms**
SA # 6	**14.D.3**	**normal subgroups**
SA # 7	**14.I.1**	**conjugate subgroups**
SA # 8	**15.C.7**	**normal subgroups**
SA # 9	**15.F.1-4**	**G/C cyclic implies G Abelian**
SA #10	**16.A.3**	**FHT_{Groups}**
SA #11	**16.F.1-6**	**1st Isomorphism Theorem (for groups)**
SA #12	**17.B.1-4 & 17.H.5**	**rings**
SA #13	**18.B.6, 18.D.6, & 18.F.2**	**ideals**
SA #14	**19.B.1**	**FHT_{Rings}**
SA #15	**20.C.1-3**	**finite rings**