

Math 351:03 — Fall 1999
MW4 SEC-217
Prof. Bumby

Workshop 12, Review of whole course.

What can be assumed? The first exercises on a topic are often designed to call attention to something that will be developed later. Since no theory exists, the proof is often long and full of technical details. Later, the details of the proof have been summarized in statements of theorems. Although you should be able to demonstrate that you can work with these details, a subject should be remembered through its main theorems. To use a theorem, you need to quote it accurately and verify its hypotheses before jumping to its conclusion. Although you frequently see shortcuts in print, they are not available to you on an exam. At this stage, you are still required to give a complete proof of everything that you claim. Even if you are not asked to prove something *from first principles*, there will be some routine verifications that should not be omitted unless you are told that it has been verified. For example, you should not assume that a set with an operation is a group unless told to do so. The whole point of the exercise may be to test your understanding of the axioms and their verification.

A reconsideration. Some results are so fundamental that they become part of the standard notation. Looking back on the result, one sometimes needs a clue to know what requires proof. For example, in the last class, we looked at Problem 34 from Section 2.4. Lots of details were given, and the proof also included most of a solution of the unassigned Problem 33. However, the proof did not use *Lagrange's theorem*, because I had forgotten that this result had been proved in this section. It would have been better to organize a proof around that result.

My approach was also a reflection of having never seen any evidence that the difficulties with Problem 12 of Section 1.4 were overcome. We can use the statement of Lagrange's Theorem to give a short proof. The saving comes from having a statement whose conclusion establishes divisibility. In Lagrange's theorem, the divisibility $m|n$ is obtained by writing a set of n elements as a disjoint union of a number of sets, all of size m . In our direct proof, divisibility was proved using the Euclidean algorithm to write $n = mq + r$ with $0 \leq r < m$. The number m was characterized as the least positive integer with a certain property, and r was shown to have the same property. This led to $r = 0$, proving $m|n$. For the abstract proof to work, the main consequences of defining property of m must be part of the theory. In particular, it is necessary to have a *group* of order n with a *subgroup* of order m in order to satisfy the hypothesis of Lagrange's Theorem.

Part of the given information was that f was an element of order p in $A(S)$. The *definition* of order of an element includes the solution of Problem 12 of Section 1.4, so it is not necessary to repeat that method of solution. This may not have been noticed since the details were left to the reader when this was introduced on p. 60 in Section 2.4. The earlier exercise shows that the least positive m with $f^m = e$ is the number of different elements of the form f^k . Now, this number is identified as the size of a set. Given $s \in S$, we defined the *stabilizer* of s to be $S_s = \{g \in A(S) : gs = s\}$. It is easy to show that this is a subgroup of $A(S)$. The left cosets of S_s are identified with the elements in the orbit of s . The first time you make this identification, a detailed proof is required. After you start using definitions that depend on this proof, the proof is almost part of the notation.

Automorphisms. Given a group G and an element $\sigma \in G$, Example 9 of Section 2.5 defined a mapping $\phi: G \rightarrow G$ by $\phi(g) = \sigma^{-1}g\sigma$. Since $\phi(gh) = \sigma^{-1}gh\sigma$ and

$$\begin{aligned}\phi(g)\phi(h) &= (\sigma^{-1}g\sigma)(\sigma^{-1}h\sigma) \\ &= \sigma^{-1}g(\sigma\sigma^{-1})h\sigma \\ &= \sigma^{-1}gh\sigma\end{aligned}$$

we see that ϕ is a group homomorphism. Since only multiplication in G was used in the definition of ϕ , products could be rearranged using the general associative law. This proof is automatically invoked whenever we refer to ϕ as the “inner automorphism induced by σ ”. Problem 26 of Section 2.5 built on this to consider the mapping from G to the group $A(G)$ of all permutations of (the underlying set of) G . The exercise asked to show that $\sigma \mapsto \phi$ is a group homomorphism. That is, the composition of mappings $\alpha = \phi_0 \circ \phi_1$ is the inner automorphism β induced by the product $\sigma_0\sigma_1$ in G . (I have changed notation on purpose.) This requires showing that $(\forall g \in G)[\alpha(g) = \beta(g)]$. Since there are so few tools available, it is not surprising that, once notation has been fully expanded, this will follow from the associative law for the operation in G . Every group homomorphism defines an important subgroup of its domain — the kernel. The second part of this asks for the kernel of this homomorphism, which is the set of elements $\sigma \in G$ for which ϕ is the identity mapping. Using the definitions, this requires $\sigma g \sigma^{-1} = g$ for all $g \in G$. The problem asks to show that this condition defines the same subset as the property $\sigma g = g \sigma$ for all $g \in G$, that defines $Z(G)$. This should *look* obvious. The proof consists of showing that the axioms of a group establish the equivalence of the two statements. The general associative law allows us to hide the details of computation in notation. If you need to emphasize the details, to show meet the standards of *proof*, you should use parentheses to identify different ways of associating an expression. Separate proofs of the two implications in an equivalence can also help to avoid the appearance of assuming the result you are trying to prove. In general, a proof should begin by using the definitions of objects in the statement, and then employing methods appropriate to the level of detail of the resulting statements.

In Problem 28 of Section 2.5, which was not assigned, the set of automorphisms of G was shown to be a subgroup of $A(G)$. This required only consideration of the behavior of compositions and inverses of automorphisms on a product of elements of G . This group was denoted $A(G)$ in Problem 34, which was assigned. That problem asked to show that the group of inner automorphisms, constructed in Problem 26, is a *normal* subgroup of this group of all automorphisms. (When you are showing something to be a normal subgroup, the fact that it is a subgroup may have already been established. That is the case here — although you need to interpret previous results to see that this is included.) Although this result is fairly difficult, a clear formulation of what is required shows the path to the solution.

Inner automorphisms play an important role in the cycle notation for S_n . If you have the cycle description of σ , and $\tau \in S_n$ is any permutation, then $\tau\sigma\tau^{-1}$ is obtained by applying τ to the description of σ . This played a role in workshop problems 9, 13, 14, and the assigned problems from Section 3.2. It is easy to determine if two elements written in cycle notation are the same. This can be described in terms of the notation rather than the permutation being represented. Disjoint cycles commute with one another, and the elements in a cycle can be *cycled* to give another description of the same permutation, but *that is all*. To describe the elements of $A(S)$ where S is ordered, you can put elements in a *normal form* in which the first cycle starts with the first element of S and follows its orbit; as long as there are more elements in S , each new cycle should begin with the first element of S that has not yet appeared.

A common application of this is to use standard methods of enumerative combinatorics to find the elements with a particular cycle structure. The characterization of inner automorphisms shows that this is also a single conjugacy class. An extension of Problem 26 of Section 2.5, which appears as Lemma 2.11.1 (not included because that section was too much of a detour), and in Problems 24 and 25 of Section 3.2, shows that the size of a conjugacy class of g is the index of the centralizer $C(g)$. This centralizer is a subgroup and must contain all powers of g , so you have two different computations of the sizes of the conjugacy classes. This together with the fact that you know the total number of elements provides enough error detection that mistakes will not be believed for long. This was done for S_4 in workshop problems. You can expect to see a question of this nature for S_5 on the final.

Direct Products. The direct product $G_0 \times G_1$ of groups G_0 and G_1 was introduced in Problem 4 of Section 2.7. Its elements are ordered pairs (g_0, g_1) where $g_0 \in G_0$ and $g_1 \in G_1$, and multiplication is defined by $(g_0, g_1)(h_0, h_1) = (g_0g_1, h_0h_1)$. You should check that this construction gives a group. The exercise asked to show the $N_0 = \{(g_0, g_1) \in G_0 \times G_1 : g_1 \text{ is the identity of } G_1\}$ is a normal subgroup of $G_0 \times G_1$. You were also asked to show that $N_0 \simeq G_0$. Wherever possible, groups should be shown isomorphic by constructing the isomorphism. In this case, maps $G_0 \rightarrow N_0$ and $N_0 \rightarrow G_0$ should immediately suggest themselves. These maps should be shown to be group homomorphisms and composition in either order shown to be the appropriate identity. Workshop problem 2 showed that the set-theoretic properties of being one-to-one or onto is equivalent to the existence of a one-sided inverse, and it is usually much easier to find the inverse than to give the set-theoretic argument. The rest of that exercise asked to show that $G_0 \times G_1/N_0 \simeq G_1$. This can be done using the isomorphism theorems by introducing a subgroup $N_1 \simeq G_1$ and showing that $N_0N_1 = G_0 \times G_1$ and $N_0 \cap N_1$ contains only the identity. In Section 2.9 we considered the case in which $G_0 = G_1$ and met a problem that studied the subgroup $T = \{(g_0, g_1) \in G \times G : g_0 = g_1\}$.

Matrix rings. The ring $M_n(R)$ of all $n \times n$ matrices with entries in a ring R is a useful example of a ring. Even if R is commutative, the full matrix ring is noncommutative for $n > 1$. Matrices are also useful for constructing examples of rings. It is often easy to find a matrix that has some property, and then any subring of $M_n(R)$ containing that matrix will contain elements having that property.

For example, if you want a solution of the equation

$$x^3 = ax^2 + bx + c,$$

you can form the 3×3 matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c & b & a \end{pmatrix}.$$

We have seen several examples of this construction in $M_2(R)$.

Polynomials and the Euclidean Algorithm. The set of all polynomials with coefficients in a field F is an important example of a ring. There is a *division algorithm* in this ring that is expressed by: given polynomials $a(x)$ and $b(x)$ with $b(x) \neq 0$, there are polynomials $q(x)$ and $r(x)$ with $a(x) = b(x)q(x) + r(x)$ and the degree of $r(x)$ strictly less than the degree of $b(x)$. In fact, $q(x)$ and $r(x)$ are uniquely determined. If $r(x) = 0$, which is allowed even if we prefer not to assign a degree to the zero polynomial, we say that $b(x)$ divides $a(x)$.

Replacing $a(x)$ by $b(x)$ and $b(x)$ by $r(x)$ and continuing the process of applying the division algorithm leads to a *Euclidean Algorithm* in which the last nonzero remainder is the *greatest common divisor* of $a(x)$ and $b(x)$. The terminology in the text is different, but the standard usage is given here. The equations obtained in this way allow the greatest common divisor of $a(x)$ and $b(x)$ to be written as a linear combination with coefficients in $F[x]$ of $a(x)$ and $b(x)$. This can be used to prove *unique factorization* in $F[x]$ by showing that every ideal in $F[x]$ is generated by an element of least degree in the ideal. Note that the linear combinations of $a(x)$ and $b(x)$ are just the elements of the smallest ideal containing both $a(x)$ and $b(x)$.

As we saw on the second exam, polynomials with integer coefficients can be interpreted as being in $F[x]$ for *any* F by identifying the positive integer n with the sum of n copies of the multiplicative identity of the field. However, because some integers may be zero in some fields, it is possible that results may depend on the field F .

The assigned problems in Section 4.5 aimed at showing that certain polynomials were irreducible over certain finite fields F . This is then used to obtain certain fields $F[x]/I$ with p^n elements for certain primes p and integers $n > 1$. A hidden tool for solving these problems is the fact that a polynomial of degree 2 or 3 is irreducible if it has no roots. This allows irreducibility to be checked for small p . One should get out of the habit of doing this before you get hurt. Not only is this limited to very low degree, but it is impractical except for *tiny* primes. Of course, for tiny primes, there are simple hand computations that allow irreducibility to be verified without a computer. However, computations in finite fields lead to important applications of Abstract Algebra to everyday life — chiefly through *coding theory* which has been used to design *error-correction* in digital representations of data as well as providing encryption for secure communication.

Difficulty of managing the data in hand computation hides the fact that the Euclidean Algorithm is an easy, fast and reliable process on a computer. When combined with the fact that every element in the field with q elements satisfies $x^q - x = 0$, one gets that there is a single Euclidean algorithm calculation that determines whether a polynomial has any factors of degree d for any d . Performing this test for d up to half the degree of a polynomial can certify that a polynomial is irreducible. The size of the field F enters only through a requirement that calculations be done with quantities that give an unambiguous representation of elements of F . This leads to bounds on time and space requirements of the computation that are bounded by a power of the logarithm of the number of elements in the field. This is much smaller than the *count* of the number of elements used in a search for a root of the polynomial.

Constructions of fields. If $f(x)$ is an irreducible polynomial of degree n over the field F , and M is the ideal of multiples of $f(x)$ in $F[x]$, then M is a maximal ideal and $F[x]/M$ is an extension field of F containing a root of $f(x)$. If this field is considered as a vector space of F (by *forgetting* all of the multiplication in $F[x]/M$ except when the first factor belongs to F), it has a basis consisting of $\{x^j : 0 \leq j < n\}$, so has dimension n . This construction was considered in Section 5.3 and plays an important role in a number of classical results towards we have aiming without actually reaching them.

On such result is the impossibility of trisecting a general angle (or, to be very specific, an angle of $\pi/3$). In outline, this is done by showing that a single construction allowed by Euclidean geometry can only introduce a point whose coordinates lie in a field extension of degree at most 2 over the field generated by the coordinates of previously known points. No sequence of such operations can lead to an element satisfying a cubic equation over the field of coordinates of initially-known points.

Another result is the impossibility of solving (most) equations of degree 5 or more by the extraction of roots. Formulas for solving equations of degree at most 4 were known since the middle of the 16th century. By the 19th century, the process of solving equations had been abstracted to the point where one could describe what happens in different methods of solving equations. The *Galois theory* drew on all of the algebra that we have been developing to show that more than extraction of roots is needed to solve equations. The key idea was to construct a field that contains *all* roots of the equation under consideration. The operation of permuting the roots leads to a group of automorphisms of this field extension, and the order of this group is equal to the degree of the field extension. If the equation can be solved by radicals, this group will contain a chain of subgroups, each one normal in the next largest subgroup with abelian quotient. However, the general equation of degree n is associated with S_n , and S_n , for $n \geq 5$ has only the alternating group as a proper normal subgroup, and the alternating group has no proper normal subgroups. There are some technical difficulties requiring that all n^{th} roots of unity be added to the field before attempting to extract n^{th} roots. This was annoying in the early days of the subject (before complex numbers), but cause no difficulty in the modern treatment. To introduce this, some lecture time was devoted to the properties of cubic equations and their solutions.

The problems dealing with extension fields should be done carefully because of their connection to important problems in the history of the subject, even if they seem to barely scratch the surface.

More on algebraic numbers. The construction of field extensions can be copied over a ring if the polynomial is *monic*, i.e., has all coefficients in the ring and coefficient of the highest degree term equal to 1. Rings obtained by extending the integers by roots of $x^2 + 1$, $x^2 - x + 5$, and $x^2 - 10$ appeared in workshop problems and $x^2 + 5$ figured in a problem on the second exam. These rings have much in common with the ring of integers. Even when they fail to have unique factorization, they have several useful properties that serve as a replacement. Although the search for unique factorization played an important role in the development of the theory of commutative rings, it is a very special property. It has become important to know how we can work around it. Computation in these rings is a lively subject, to which we have given only a brief introduction.

The abstract approach leads to a very easy way to write an equation satisfied by sums and products of algebraic numbers whose defining equations are known. Problem 7 in Section 5.3 is a very simple example of this — perhaps too simple. In general, one should look for a polynomial whose degree is the product of the degrees of the numbers being combined. However, in return for accepting a large degree, you get a very simple description of the polynomial.