Some Thoughts on Algebra Teaching*

Mark Wildon

August 2000

The purpose of this essay is to give some of my thoughts on the tricky question of choosing how abstractly, and in what generality, algebra teaching should be approach. I suggest that is perhaps some needless abstraction in undergraduate algebra courses. That said, I also argue that there are also instances where a more general or abstract approach would be beneficial. As a specific example I look at some of the ways one can teach quotient groups.

I hope that few of my lecturers would deliberately choose to explain things in a way they believed sub-optimal[1]. This leads to the inescapable conclusion that some of them really *did* believe:

- That the best way to explain direct sums of vector spaces to a predominately 1st year undergraduate audience was via universal algebra homomorphisms.
- That it is possible, and indeed desirable, to spend three lectures defining the derivative of an $\mathbb{R}^n \to \mathbb{R}^m$ function without giving any examples.
- That the correct way to introduce the determinant is as a scaling factor between volume forms τ and $\tau\phi$ on a vector space V, where ϕ is an endomorphism of V. (Rather than as a volume form itself or in some even more elementary way).
- That one was legitimately entitled to express extreme surprise on learning the news that category theory is not generally lectured to Cambridge undergraduates.

but also they, or perhaps the syllabus setters, believed:

- That explaining how linear maps $\mathbb{R}^n \to \mathbb{R}^m$ are represented by matrices was made easier to follow by first restricting to the case $n = m = 3$ and then writing out explicitly almost a page of sums.
- That there is no need to have a course on modules in the undergraduate Tripos. Thus two different lecturers were forced to spend many hours independently proving Jordan's Normal form and the structure theorem for abelian groups[2].

---

*Originally the devastating critique of Cambridge algebra teaching long promised on my website. I hope most of the vitriol has been removed. Unfortunately most of the pretension seems to remain.

[1] Although several might have left you wondering.

[2] If you didn't take the Maths Tripos in Cambridge in recent years then you'll have much more chance of knowing both of these are pretty trivial consequences of the structure theorem for modules over a PID

You may well agree with some of these sentiments. It is even possible that you think that every one exemplifies a patently correct method of teaching. However I hope you will agree with me that in at least some of them the level of abstraction has been pitched either too high, or too low for its intended audience.

'To each his own level of abstraction' is an excellent maxim, but one that creates an obvious difficulty for teachers and lecturers. Sometimes ones approach is essentially governed by a choice of how generality, and how abstractly one wants to look at the problem. Also, although it is desirable to go over things in different ways (perhaps by changing the level of abstraction), in a lecture time constraints make this difficult. Thus my argument is that in good algebra teaching, the level of abstraction demands to be chosen with great care.

To illustrate this point I present three different approaches to teaching the notion of quotient groups. I choose this example mainly because it lends itself well to my argument and I want to present a new (or old and forgotten) way of teaching it. Also many of my friends who attended algebra teaching in their 1^{st} year found quotients groups their first major difficulty. Sometimes the difficulty proved insurmountable.

Firstly I present a very standard approach, as can be found with at most minor variations in many undergraduate textbooks. The account here is drawn verbatim from Dr Tom Körner's handout for the Cambridge course C1/C2 Algebra and Geometry (from which I originally learnt group theory and much else besides). It is rather awkward for me that to make my points I need to pick on a specific example of this kind of approach — by choosing this one I cannot at least be accused of deliberately presenting a poor exposition in order to give my arguments more weight.

At the point we join the text, groups, subgroups and homomorphisms have been defined, Lagrange's theorem, Cayley's theorem, and the Orbit-Stabiliser theorem have been proved and many standard examples have been given.

---

10 A brief look at quotient groups

The notion of a quotient group (like the notion of quotients in general) is extremely useful but also fairly subtle.

If we consider a group G with a subgroup H then it is natural to try and put a group structure on the collection of left cosets gH. The 'natural definition' is to write $g_1H.g_2H = g_1g_2H$. BUT THIS DOES NOT ALWAYS WORK.

Theorem 91 *Let G be a group and H a subgroup of G. The following two statements are equivalent*

(i) $g_1H = g_1'H,\ g_2H = g_2'H \ \Rightarrow g_1g_2H = g_1'g_2'H$,

(ii) $ghg^{-1} \in H$ whenever $g \in G,\ h \in H$.

[**Proof:** (Proofs were not included in the handout).

Assume (i). Let $g \in G, h \in H$. Then since $hH = eH = H$ we can apply (i) to get $hH.gH = eH.gH$. By the definition of coset multiplication this means $hgH = gH$. Left multiplying by g^{-1} tell us $g^{-1}hg \in H$ which implies (ii).

Assume (ii). Then $g_1H = g_1'H$ implies $g_1 = g_1'h_1$ for some $h_1 \in H$. Similarly $g_2 = g_2'h_2$ for some $h_2 \in H$. Thus $g_1g_2H = g_1'h_1g_2'h_2H = g_1'g_2'{g_2'}^{-1}h_1g_2'H = g_1'g_2'H$ where we used (i) to show that that ${g_2'}^{-1}h_1g_2'$ lies in H. Thus (ii) implies (i). $\square$]

In view of this we make the following definitions.

Definition 92 *If H is a subgroup of a group G we say that H is* normal *if $ghg^{-1} \in H$ whenever $g \in G$, $h \in H$.*

This is sometimes restated as 'H is normal if $gHg^{-1} \subseteq H$ for all $g \in G$'.

Lemma 93 *Let H is a subgroup of a group G. Then H is normal if and only if $gH = Hg$ for all $g \in H$.*

[This is very easy to prove. It is also not hard to prove the stronger result that H is normal if and only if the set of left cosets is equal to the set of right cosets *as sets*.]

Since left and right cosets agree for H normal we shall refer, in this case, to 'cosets' rather than left cosets.

Definition 94 *If H is a normal subgroup of a group G the set G/H of cosets gH with multiplication defined by $g_1H.g_2H = g_1g_2H$ is called a quotient group.*

Theorem 95 *Quotient groups are groups.*

[The real being that quotient groups are well-defined. Showing from this that elements of the quotient group have inverses and that there is an identity element is trivial.]

I reiterate the warning above:

$\boxed{\text{QUOTIENT GROUPS EXIST ONLY FOR NORMAL SUBGROUPS.}}$

Dr Körner goes on to give examples of normal subgroups and quotient groups. He then discusses the quotient homomorphism and proves the 1st isomorphism theorem.

Let me stress once more that I think this is an excellent account of a tricky subject. However, despite its clarity, quotient groups were a major source of difficulties for people taking the course. I think once of the main reasons for this was that in the standard exposition, one first 'secretly' defines the quotient group (by giving what will be the definition of coset multiplication) and then proves that it is well defined (via the lemma). This sort of approach is apt to cause confusion to those not used to it. For example I think many people overlook the need to prove that the quotient group really is a group. After all if the lecturer, looked up to as a God-like intelligence by most of the audience, defines something whose name strongly suggests that it is a group, what more need be said? Thus the theorem 'Quotient groups are groups' seems very mysterious, the confusion arising because of the inversion of the familiar order.

Secondly I would argue that really there is not so much motivation for the approach. What is so 'natural' about the proposed multiplication of cosets? There is a far more obvious way to multiply cosets — two cosets g_1H and g_2H are subsets of the group G and could just be multiplied elementwise. Later I will prove the theorem:

Theorem *Let H be a subgroup of G. Define the product of two cosets g_1H and g_2H to be the subset of G given by multiplying each element of g_1H by each element of g_2H. That is,*

$$g_1H \, . \, g_2H = \{x_1x_2 | x_1 \in g_1H, x_2 \in g_2H\}$$

Then the product of two cosets is always another coset if and only if H is a normal subgroup of G. If so, $g_1H \, . \, g_2H = (g_1g_2)H$ for all $g_1, g_2 \in G$.

This theorem (whose proof is perhaps even more straightforward than the proof of the lemma above) seems to suggest this is the more natural way to define coset multiplication. The immediate corollary is the definition of a quotient group, it being obvious that it is well-defined.

At more advanced levels it is very frequently the case that one first makes the definition, then shows it is well-defined. The alternative is a long chain of motiveless results finally leading to the definition. Both of these can be objected to. For example, consider how we might approach defining the simplicial homology groups of a manifold. The more traditional approach is to undergo a long excursion into piecewise topology, prove certain rather technical results about complexes of abelian groups, and finally present the definition secure in the knowledge it is well-defined. The alternative is to give axioms (for example the Eilenberg-Steenrod axioms) that the homology groups must satisfy and then to show (perhaps after working with the axioms for a while to gain familiarity) that there really is an object with the required properties. The latter approach is undeniably more abstract but to some at least it may seem simpler. Certainly it has the advantages of emphasising the connections with other homology theories.

Next I present a different approach to quotient groups whose highlight is the theorem mentioned above. Rather than write a whole chapter (or even a chapter of one) I have indicated where standard examples and theorems should be inserted — I assume the reader will be able to fill in the gaps! Proofs are however given in full. Please assume that as in the extract from Dr Körner's handout, groups, subgroups and homomorphisms have been defined and some of the usual examples have been given.

Definition 1 *A* semigroup *is a set X with an associative law of composition $(*)$.*

Every group is a semigroup and a semigroup is a group if and only if it has an identity element and every element has an inverse. Most of the semigroups we will look at will have an identity element. Semigroups are in some ways like groups. For example we can consider subsemigroups of a semigroup just as we considered subgroups of a group.

Lemma 2 *Let X be a semigroup. Then if X has an identity element it is unique.*

Proof: (Exactly the same proof as for groups). Suppose e and e' are identity elements. So $e * x = x * e = x$ and $e' * x = x * e' = x$ for all $x \in X$. Put $x = e'$. We obtain $e = e * e' = e'$. $\square$.

Example 3 *Examples of semigroups and subsemigroups. Include an example without an identity element (for example the ring of $(n \times n)$ matrices under multiplication). A subsemigroup of this is the group of invertible matrices.*

Theorem 4 *Given a group G let $P(G)$ be the power-set of G. Thus the elements of $P(G)$ are subsets of G and $|P(G)| = 2^{|G|}$. We can turn $P(G)$ into a semigroup by defining for $A, B \subseteq G$:*

$$A * B = \{ab \,|\, a \in A, b \in B\}$$

Proof: Multiplication in $P(G)$ inherits associativity from multiplication in G; if $A, B, C \subseteq G$ then:

$$\begin{aligned} A * (B * C) &= \{a(bc) \,|\, a \in A, b \in Bc \in C\} \\ &= \{(ab)c \,|\, a \in A, b \in Bc \in C\} = (A * B) * C\,. \end{aligned}$$

Also, if $e \in G$ is the identity element of G, $\{e\}$ is the identity element of $P(G)$. $\square$

Example 5 *i) For any group G and any subset $X \subseteq G$, $G * X = X * G = G$ and $G * \emptyset = \emptyset * G = \emptyset$*

ii) If H is a subgroup of G then $P(H)$ is a subsemigroup of $P(G)$.

iii) Multiplication in $P(G)$ is commutative (i.e. $A * B = B * A$ for all $A, B \subseteq G$) if and only if G is abelian.

Definition 6 *Let H be a subgroup of G. Then the* left cosets *of H in G are the subsets $\{g\} * H$ as g runs over G.*

Since $\{g\}$ is a singleton set we will write gH rather than $\{g\} * H$. Thus $gH = \{gh \,|\, h \in H\}$. Cosets give us an important handle on the structure of groups.

Lemma 7 *i) Every coset has exactly $|H|$ elements.*

ii) Two cosets g_1H and g_2H are either equal or disjoint. They are equal if and only if $g_1g_2^{-1} \in H$.

iii) There are precisely $|G| \,/\, |H|$ distinct cosets.

iv) (Corollary) Lagrange's Theorem: if H is a subgroup of G then $|H| \,\big|\, |G|$ $\square$

It sometimes happens that the product of two cosets is another coset. Of course this product takes place in the semigroup $P(G)$ — that is why we defined it! For example if G is abelian then it is easy to check that $g_1H * g_2H = (g_1g_2)H$. However it is not necessary for G to be abelian for this to happen as the following example shows:

Example 8 *Let $G = S_3 = \langle \tau, \sigma \,|\, \tau^2 = \sigma^3 = e, \tau\sigma = \sigma^{-1}\tau \rangle$ and let $H = \langle \sigma \rangle$. Then there are precisely two different cosets of H in G, $H = \{1, \sigma, \sigma^2\}$ and $\tau H = \{\tau, \tau\sigma, \tau\sigma^2\}$. The product of any two cosets is another coset: $H * \tau H = \tau H * H = \tau H$ and $H * H = \tau H * \tau H = H$.*

The theorem below which is the crux of the whole matter gives a necessary and sufficient condition for the product of two cosets to be another coset.

Theorem 9 *The product of two cosets is always another coset if and only if for every $g \in G$, $gHg^{-1} \subseteq H$. As usual, gHg^{-1} is shorthand for $\{g\} * H * \{g^{-1}\}$. If this is the case, $g_1H.g_2H = (g_1g_2)H$ for all $g_1, g_2 \in G$.*

Proof: Given two cosets g_1H, g_2H we can *always* form their product in $P(G)$:

$$\begin{aligned} g_1H * g_2H &= \{g_1h_1g_2h_2 \mid h_1, h_2 \in H\} \\ &= \{g_1g_2(g_2^{-1}h_1g_2h_2 \mid h_1, h_2 \in H\} \\ &= \{g_1g_2kh \mid k \in g_2^{-1}Hg_2, h \in H \end{aligned}$$

Thus $g_1H * g_2H$ is a coset if $k \in H$ for every $k \in g_2^{-1}Hg_2$. This proves the 'if' part.

If $k \in g_2^{-1}Hg_2$ is not in H then $g_1H * g_2H$ contains g_1g_2k and in addition all the elements of the coset g_1g_2H. But we know every coset of H has size $|H|$ (Lemma 7) so the product cannot be a coset. This shows the 'only if' part. □

Definition 10 *If H is a subgroup of G such that $gHg^{-1} \subseteq H$ for every $g \in G$ we say H is a* normal *subgroup of G.*

Theorem 11 *Let H be a normal subgroup of G. Then the set of cosets of H in G is a subgroup of the semigroup $P(G)$.*

Proof: All the work is done for us by Theorem 9 which tells us the set of cosets is closed under multiplication. H is the identity since $gH * H = H * gH = gH$ (using theorem 9) and the inverse of gH is $g^{-1}H$ since $gH * g^{-1}H = g^{-1}H * gH = H$ (again using theorem 9). □

Definition 12 *If H is a normal subgroup of G then the set of all cosets of H in G with the product inherited from $P(G)$ is called the* quotient group *of G by H. It is written G/H. We know there are $|G| / |H|$ cosets of H in G so $|G/H| = |G| / |H|$.*

It would of course be quite possible to present our key result (Theorem 9) without ever mentioning semigroups. This would cut the length down considerable. However by looking first at semigroups students will hopefully see $P(G)$ in a more general context as well as get extra practice in working with it. Some exercises on this approach are given at the end. In any case it is worth looking at semigroups for their own interest. For example, the transition matrices $\mathbf{P}_t$ for a continuous time Markov process form a semigroup; the Chapman-Kolmogorov equations give the multiplication: $\mathbf{P}_{s+t} = \mathbf{P}_s\mathbf{P}_t$. There are of course many other examples in algebra alone.

Lastly we consider how we might look at the matter from a more rarified height of abstraction. There are many pitfalls if this is attempted as the first approach. Consider the following dialogue, between **CT**, a 24^{th} Century category theorist and **U**, an everyman-like figure designed to evoke a late 20^{th} Century undergraduate.

U: What's a quotient group? (Our subject has an inquiring mind)

CT: Well, no doubt the best way to look at quotient groups is as a certain universal object in the category of groups. You are, of course, familiar with the concept.

U: No.

CT: What? But surely you are familiar with the basics of category theory?

U: I don't think we've done that yet.

CT: Impossible!

Of course it is easy to heap ridicule on category theory. We are all category theorists at heart and most of us self-loathing to some degree of other. To the right audience, the sort of approach our friend **CT** is aiming for might be quite illuminating. The example below is aimed at this 'right audience'. As before maps are multiplied on the left (since we are doing category theory and not algebra).

Theorem 13 *If N is a normal subgroup of G then the projection $\rho : G \to G/N$ is a universal element for the functor f :* **Grp** $\to$ **Set** *which assigns to each group G the set fG of homomorphisms $f : G \to H$ that kill N.*
Discussion: A slightly less formal restatement is 'If N is a normal subgroup of G then the quotient group G/N is universal for group homomorphisms $G \to H$ that kill N'. All either of these grand phrases mean is that every homomorphism $\theta : G \to H$ with $N \subseteq \ker \theta$ factors uniquely through the projection ρ. That is $\theta = \phi\rho$ for a unique homomorphism $\phi : G/N \to H$. This is easily proved. Note also that $\ker \phi = \ker \theta N$ and $\operatorname{im} \phi = \operatorname{im} \theta$ (this is totally formal).

From this universal property of the quotient group G/N it is easy to deduce all the isomorphism theorems. As an exercise we deduce third isomorphism theorem: if $N \subseteq H$ and $N, H \trianglelefteq G$ then $(G/N)/(H/N) \cong (G/H)$. The map $G \to G/H$ kills H so certainly it kills N. By the universal property it induces a map $G/N \to G/H$ which kills H/N. Applying the universal property once more gives the required isomorphism: $(G/N)/(H/N) \cong (G/H)$

It should be obvious that nothing very profound is happening - all we are doing is writing out the standard proofs. However, when the standard proof says 'by the first isomorphism theorem' we say 'by the universal property'. The real point is that the paragraph above is also a proof of the same third isomorphism theorem for rings, modules, vector spaces, algebraic groups, on so on. (Of course in each case we have to first establish that a suitable universal object exists!)

Perhaps the most important point is that as a universal object is unique up to isomorphism, we are free to use any construction of G/N that we like, but then to look at it whatever way suits our present purpose best. Amusingly enough it is actually possible to give a construction of G/N that never mentions cosets (it does however use some fairly heavy category theory). The interested reader is referred to MacLane's book (*Categories for the Working Mathematician* p57 and pp120-125).

We have now seen three different ways of looking at quotient groups. Arguably the second is more abstract than the first (given that it uses semigroups extensively). On the other hand it avoids the problems mentioned above concerning proving well-definedness and leads to a perhaps more natural definition. So here we may have an example where more abstraction led to an easier exposition. I hope we are all agreed that the third approach has its points but is not the best way to introduce the subject for the first time!

It can be easier to go from the concrete to the abstract. However the assumption that this is always the case deserves questioning. For example, in Cambridge concrete groups, that is, subgroups of the group of functions $f : X \to X$ for some set X, are introduced before abstract groups. My experience is that this leads to some confusion. For one thing, any previous contact (for example at A-level) with groups is almost certain to be with abstract groups[3]. For another, I am by no means convinced concrete groups are an easier concept to grasp than abstract groups.

[3]SMP A-Level Maths would for example leave you with the impression group theory consisted entirely of the intensive study of S_3 and the construction of group multiplication tables.

Another example from Cambridge, already hinted at, is that due to the lack of a course on modules lecturers end up proving over and over again special cases of the decomposition theorem for modules over a PID. To some extent this may be no bad thing but when the list of courses clearly affected runs to at least five (Linear Mathematics, Groups Rings & Fields, Number Fields, Representation Theory and Algebraic Curves) one has to wonder if the omission can be justified, even on the grounds of avoiding possibly redundant abstraction. Redundant from the point of view of the Cambridge syllabus of course.

A lot of what I have said applies to the problem of choosing definitions. Naturally one of the main criteria is what previous work can be counted as prerequisite knowledge. However there are others. For example, here is the standard definition of a group:

Definition *A group is a set G together with an operation $*$ such that*

i) If $a, b \in G$ then $a * b \in G$. (Closure)

ii) If $a, b, c \in G$ then $(a * b) * c = a * (b * c)$. (Associativity)

iii) There exists an element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$. (Identity)

iv) If $a \in G$ there is an element $a^{-1} \in G$ with $a^{-1} * a = a * a^{-1} = e$.

This definition could be made slightly stronger, for instance, by insisting that the identity element be unique. As we know, uniqueness of the identity is a consequence of the existing axioms so it would be redundant to state it along with them. There is already considerable redundancy though. Below is a minimal definition of a group (minimal in the sense that no requirement can be weakened if every object it defines is to be a group):

Definition *A group is a set G together with an operation $*$ such that*

i) If $a, b \in G$ then $a * b \in G$. (Closure)

ii) If $a, b, c \in G$ then $(a * b) * c = a * (b * c)$. (Associativity)

iii) If $a, b \in G$ then the equation $a * x = b$ has a solution $x \in G$ and the equation $y * a = b$ has a solution $y \in G$. (Equations are soluble)

It is not hard to check that these axioms imply that there is a unique identity element and that the x and y of axiom (iii) are equal. Other minimal definitions are possible; one could for example insist on a left identity, a right identity (trivially the same) and left (but *not* right) inverses. Possibly it is more elegant to give a definition with no redundancy: that said an asymmetric definition such as the above will never be elegant. In any case, I think these examples show that for the purposes of teaching it can often be better to give a full definition, albeit a redundant one. A definition should appeal to one's existing intuition about what it is defining, just as a lecturer should ideally appeal to his audience's knowledge and not his own.

MARK WILDON

Three exercises on the semigroup definition of quotient groups are given below.

Exercise 1 *Find every subgroup of $P(G)$. Are they all of the form H/K for $K \trianglelefteq H \leq G$. (It is conventional to write $H \leq G$ to mean H is a subgroup of G and $K \trianglelefteq H$ to mean K is a normal subgroup of H.)*

Exercise 2 *If H is a (not necessarily normal) subgroup of G what is the smallest semigroup that contains all the cosets of H?*

Exercise 3 *Think about one could define quotient rings in an analogous method. We now have a* ring *of subsets of our ring R. If I is an ideal we need to consider those subsets of the form $r + I$ and show they form a ring. Less seems to be gained by this approach than was the case for groups.*