School of Mathematics University of New South Wales

MATH3711: Higher Algebra (2007,S1)
Assignments and Mathematical Writing [1]

For many of you, Higher Algebra will be the first serious pure mathematics course you will take. Unlike second year courses, the majority of questions you will be asked to do will involve proofs (gone are the days where you need only follow an algorithm to do well!).

One of the hardest things for beginning third year maths students is learning to write proofs and more generally, to write in good mathematical style. This is complicated by the fact that mathematics is often communicated orally in a very different manner to how it is communicated when written. Indeed, you will find that the lecture notes are written differently from how you are expected to write your assignments. The lecture notes will be written from a pedagogical point of view. Your assignments should be written with complete mathematical rigour. For each assignment, a portion of the mark will be assigned to mathematical writing. Below are some tips on good mathematical writing.

- Make sure you explain any new symbols you introduce. For example, the symbol G will almost invariably represent of group in this course, nevertheless, if it doesn't appear in the question you are working on, you should write something like, "Let G be a group ...".
- Don't just show working. Lines of equations are fine but usually (though not quite always) require a sentence or two explaining the logical role they play in your argument/proof.
- Make sure the logic of your argument is clear. If it is clear, it should be very easy to check the veracity of your argument. This ease of checking is one of the things you should aim for. Whenever you claim some fact (and this will typically be in every sentence), you should make sure it follows from either simple logic, definitions given in class or results given in class. If it follows from a theorem or definition, it is often a good idea to write "By definition" or "By theorem X" so the reader knows where you are drawing your conclusions from and thus follow and check your argument easily.

The best way to improve your mathematical writing style is to read well-written proofs in good maths texts. I will help you out in tutorials but, to kick you off, I have included below some sample proofs. They will be referred to in lectures 2 and 3, when they will make more sense. The remarks in parentheses have been added to help you understand the proof.

Proposition 1 *Inverses in a group are unique.*

Proof. We start by making a more precise statement of the proposition. Let G be any group and $g \in G$ an arbitrary element of G. Suppose h and h' are inverses of g in the sense that $gh = hg = 1$ and $gh' = h'g = 1$. The proposition states that $h = h'$ and that is what we are required to show. (Check to make sure you understand this!)

Using group axioms we indeed find $h = h1 = hgh' = 1h' = h'$. Hence, inverses in a group are unique.

[1] by Daniel Chan

Proposition 2 *Let S be a finite set and g be a permutation of S. There exist subsets $S_1, \ldots, S_k$ of S (for some integer k) such that i) for each $i \in \{1, \ldots, k\}$, g permutes the elements of S_i cyclically and ii) S is the disjoint union of the S_i as i varies from 1 to k.*

Proof. We let the S_i be the distinct subsets of the form $S(a) := \{a, g(a), g^2(a), g^3(a), \ldots\}$ where a is any element of S. (Note, we force the S_i to be distinct by ignoring any repeats which may occur if $S(a) = S(b)$ for elements $a, b \in S$. Also, the notation $:=$ means "is defined to be equal to"). Note that the union of the S_i is indeed S as given any $a \in S$ we have $a \in S(a)$. Given any $a \in S$, we check g permutes the elements of $S(a)$ cyclically. Since S is finite, there must be an equality of the form $g^j(a) = g^{j+d}(a)$ for some non-negative integer j and positive integer d. We may choose such an equality with d minimal so that $\{g^j(a), g^{j+1}(a), \ldots, g^{j+d-1}(a)\}$ are all distinct. (Make sure you know why you can choose d minimal). Hence, $a = g^{-j}g^j(a) = g^{-j}g^{j+d}(a) = g^d(a)$ and $a, \ldots, g^{d-1}(a)$ are all distinct too. Indeed, if there were an equality $g^p(a) = g^q(a)$ with $0 \leq p, q < d$ then permuting by g^j would give us the contradiction $g^{j+p}(a) = g^{j+q}(a)$. Now for any integer n we write $n = md + r$ where $0 \leq r < d$. Then $g^n(a) = g^r(a)$ and hence the elements of $S(a)$ are $a, g(a), \ldots g^{d-1}(a)$ and g permutes these elements cyclically.

It remains only to show that the subsets S_i are disjoint. By the way we defined the S_i, this amounts to proving that if $S(a)$ and $S(b)$ intersect non-trivially for some $a, b \in S$, then $S(a) = S(b)$. Suppose indeed that there are positive integers p, q with $g^p(a) = g^q(b)$. Then $S(a)$ contains $S'(b) := \{g^q(b), g^{q+1}(b), \ldots\}$. Since $b = g^e(b)$ for some positive integer e, we find that $S'(b) = S(b)$ and hence $S(b) \subseteq S(a)$. Arguing symmetrically gives the reverse inclusion so indeed $S(a) = S(b)$. This completes the proof of the proposition.

You may think proofs such as the one above are terse and lose a lot of the mathematical intuition. Proofs are often not designed with pedagogy in mind. They are usually designed so that you can check easily all the steps and check that there are no gaps in logic. Nevertheless, a good proof will achieve this and also be close to one's mathematical intuition.