How to prove stuff: the game of Abstract Algebra

Treat Abstract Algebra as a game. This game comes with an ever-expanding set of rules. You must play by the rules, otherwise the referee (that’s me) will call a foul and disqualify you.

When the game begins, the only rules you have are those you learned in Math 290. You know some basic proof techniques: direct proof, proof by contradiction, proof by induction, some basic facts about sets.

The Abstract Algebra rules you have learned so far are these:

- the Well-Ordering principle
- the Quotient Remainder Theorem
- the definition of divisibility
- a theorem which describes the greatest common divisor of \(a\) and \(b\) as the smallest positive linear combination of \(a\) and \(b\)
- a theorem which says that \(\gcd(a, b) = 1\) if and only if a positive linear combination of \(a\) and \(b\) produces 1
- the definition of relatively prime integers
- a theorem which says \(\gcd(a, b) = 1\) and \(a|bc\) implies \(a|c\).

By now you have played a few rounds of the game with an experienced player (me) and have seen how to prove, for example, that every odd integer \(n\) satisfies \(n^2 = 8k + 1\) for some integer \(k\). You are now ready for some advanced tips:

Every proof has a logical structure which you should be able to block out with very little effort. Here is one of many possible forms:

**Theorem:** \(A\) implies \(B\).

**Proof:** \(A\) has a definition. \(B\) has a definition. Assuming that \(A\) is given, use any definitions and theorems at your disposal to show that \(B\) must also be true. QED

**Example:**

**Theorem:** If \(n\) is an odd integer which is not divisible by 3, then \(n^2\) has remainder 1 after division by 6.

**Proof:** \(A\) is the statement “\(n\) is an odd integer which is not divisible by 3.” \(B\) is the statement “\(n^2\) has remainder 1 after division by 6.” Since we are not new at playing this game, we know that it will be advantageous to use the Quotient-Remainder Theorem with \(b = 6\). We know that \(n\) has one of 6 possible forms: \(6k + 0, 6k + 1, 6k + 2, 6k + 3, 6k + 4,\) or \(6k + 5\). Since \(n\) is odd and not divisible by 3, we can throw out some of these forms, leaving \(6k + 1\) or \(6k + 5\). We’ve extracted all the information we can out of \(A\). To prove \(B\), square each of these forms:

\[(6k + 1)^2 = 36k^2 + 12k + 1 = 6p + 1,\]
\[(6k+5)^2 = 36k^2 + 60k + 25 = 36k^2 + 60k + 24 + 1 = 6q + 1.\]

So we know that \(n^2\) has remainder 1 and \(B\) holds. Done.

From here on out, the rules of the game expand as follows: more definitions and more theorems. Moreover, your experience grows the more you play the game, which you should use to your advantage. How to gain this experience: pay attention and take notes in lecture, read my notes, do the homework very carefully, come to office hours!

**Rule Violations:** (1) Making any statement in the course of a proof that has no justification by previously established definitions and theorems. (2) Begging the question (assuming what you want to prove instead of proving something). (3) Changing the question. I as the referee will call a foul in the event of a rule violation. Here’s an example:

**Theorem:** Every odd integer must be of the form \(6k + 1\) or \(6k + 3\) or \(6k + 5\).

**Proof:** \(6k + 1 = 2(3k) + 1\), therefore \(6k + 1\) is odd. \(6k + 3 = 2(3k + 1) + 1\), therefore \(6k + 3\) is odd. \(6k + 5 = 2(3k + 2) + 1\), therefore \(6k + 5\) is odd. QED

**The Rule Violation:** Changing the question. The proof given demonstrates only that \(6k + 1, 6k + 3,\) and \(6k + 5\) are odd numbers. It does NOT demonstrate that EVERY odd number has one of these three forms. You must first show that EVERY odd number has one of the 6 forms \(6k + r\) where \(r = 0, 1, 2, 3, 4, 5\) (Justification: Quotient-Remainder Theorem). Then you must show that we can throw away the \(r = 0, 2, 4\) terms, leaving the \(r = 1, 3, 5\) terms.

You will find that the same rules apply to the Game of Real Analysis and, more generally, the Game of Mathematics. The theorems and definitions may vary from one version of the game to another, but the logic is universal. The Games of Physics, Biology, and other experimental sciences have a wider rule set than the Game of Mathematics (plausible arguments based on observation are allowed where no absolute proof is possible, only hypotheses supported by data). The Games of Computer Science and Engineering also have wider rule sets (if a design seems to work on the first 100 million tries, or with a very high probability, it is judged reliable). Please restrict yourself in this course to the rules of the Game of Abstract Algebra.