MATH 3163 Introduction to Modern Algebra
More about Homework and Proofs

Stringing equations together is how mathematicians write, but the order of the equalities is very important. Here is the statement and proof from the course syllabus.

Let f, g, h and i be integers. If f divides h and g divides i, then fg divides hi.

PROOF: Assume f divides h and g divides i. Then there are integers r and s such that $h = fr$ and $i = gs$. Thus $hi = (fr)(gs) = f(r(gs)) = f((rg)s) = f((gr)s) = f(g(rs)) = (fg)(rs)$. Therefore, fg divides hi.

In the proof above we "know" $hi = (fr)(gs)$ by substitution. We do not directly know that $hi = (fg)(rs)$, but we do know that by successive applications of the associative property of multiplication that $(fr)(gs) = f(r(gs)) = f((rg)s)$. Also multiplication of integers is commutative so $rg = gr$. Using both properties we obtain the following string of equations:

$$hi = (fr)(gs) = f(r(gs)) = f((rg)s) = f((gr)s) = f(g(rs)) = (fg)(rs).$$

What you care about in this proof is showing hi is an integer multiple of fg. So start the string of equations with $hi =$. Any of the following three products can be on the right side of this $=$: $(fr)(gs)$, $(fr)i$, or $h(gs)$. The first is the best choice. We eventually want to transform the right hand side to "$(fg) \cdot (some\, integer)$", but need to show how it is done.

Basic scheme for doing a "proof" of an "IF..., THEN..." statement

Here is another fairly simple statement to prove about integers. We will go through the steps of the proof one sentence at a time. The GCD Theorem, Divisor Theorem and the GCD=1 Theorem are on the back of the first set of homework problems.

(P) Let a, b, d, r and s be integers. If $a = dr$, $b = ds$ and $d = gcd(a, b)$, then $gcd(r, s) = 1$.

Step 1: Change the word "IF" to "ASSUME" continue with the exact statement that follows "IF" until you get to the comma before the "THEN", change the comma to a period and **STOP**. This is the entire first sentence of your proof. **Do not write anything else in this sentence.**

Step 1 for (P): Assume $a = dr$, $b = ds$ and $d = gcd(a, b)$.

Step 2: For the second sentence (and in some cases the third one too), write down whatever useful equations (or other conclusions) you can based on either definitions of the terms used in the first sentence or on previously proved theorems or exercises–and for theorems/exercises **you must say which one(s) you are using**. Also remember to say what the new letters represent. For the first few weeks, every letter will represent an integer. But later on they may represent something else.

Step 2 for (P): Then by the GCD Theorem, $d > 0$ and there are integers f and g such that $d = af + bg$. [All we use in this proof is $d > 0$.]

Step 3: Once you have applied the definitions/theorems/exercises to get some new equations (or other information), do something with them. So, what do you do? Try stuff until you find something useful–but in the proof don't mention what didn't work. At this point, it is often useful to take a look at what you are supposed to prove happens. Then try backing up one step from what the conclusion is supposed to be, in other words check theorems, previous homework problems and definitions to see what is enough to make the required conclusion. *The most important thing to remember: This is an algebra class so* **substitution** *is your friend.* In this particular problem we are asked to prove the gcd of r and s is 1. So if you can't think of anything else at this point give $gcd(r, s)$ a name – without saying it is 1, you aren't allowed to say it is 1 until you have proved it is 1.

Step 3 for (P): Let $e = gcd(r, s)$. Then by the GCD Theorem $e > 0$ and there are integers k and m such that $r = ek$ and $s = em$.

Step 4: Repeat Step 3 using these new equations – again try substituting and manipulating until you find something useful (perhaps based on previous theorems, and previous proofs).

Step 4 for (P): Since both d and e are positive integers, $1 \leq e$ and $d \leq de$. By substitution $a = dr = dek$ and $b = ds = dem$. Thus de divides both a and b. Hence de divides d by the GCD Theorem. Since both d and e are positive integers, $de = d$ by the Divisor Theorem. Another application of the Divisor Theorem yields $1 = e$. Therefore $gcd(r, s) = e = 1$.

Here is a very complete (way too complete) proof of the statement above. It differs from the previous one by using the equation $d = af + bg$ but not using $e = gcd(r, s)$.

Assume $a = dr$, $b = ds$ and $d = gcd(a, b)$. Then by the GCD Theorem there are integers f and g such that $d = af + bg$. Thus by substituting dr for a and ds for b, we have $d = (dr)f + (ds)g$. By the associative property of multiplication $(dr)f = d(rf)$ and $(ds)g = d(sg)$. So by substituting $d(rf)$ for $(dr)f$ and $d(sg)$ for $(ds)g$, we have $d = d(rf) + d(sg)$. By subtracting d from both sides and substituting $d \cdot 1$ for d, we have $0 = d - d = d(rf) + d(sg) - d \cdot 1$. By factoring out the d using the distributive property, we get $0 = d[(rf) + (sg) - 1]$. Since $d = gcd(a, b)$, it is a positive integer by the GCD Theorem. Also, rf, sg, $rf + sg$ and $rf + sg - 1$ are integers since r, f, s and g are integers and the product of two integers is an integer and the sum of two integers is an integer and the difference of two integers is an integer. Thus we must have $0 = rf + sg - 1$ since a product of two integers being 0 implies at least one of them is 0 and we know d is a positive integer, so it is not equal to 0. By adding 1 to both sides, we obtain $1 = rf + sg$. Since $r = r \cdot 1$ and $s = s \cdot 1$, 1 divides both r and s. We also know that 1 is a positive integer. Therefore using that statement (3) of the GCD Theorem implies statement (5) of the GCD Theorem, we have that $gcd(r, s) = 1$.

NO ONE WANTS TO READ A PROOF LIKE THE ONE ABOVE!

Better version of the previous proof:

Assume $a = dr$, $b = ds$ and $d = gcd(a, b)$. Then by the GCD Theorem, $d > 0$ and there are integers f and g such that $d = af + bg$. Thus $d \cdot 1 = d = af + bg = drf + dsg = d(rf_sg)$. Hence $1 = rf + sg$ by the Divisor Theorem. Therefore $gcd(r, s) = 1$ by the GCD=1 Theorem.

Your basic approach to actually writing a proof (once you have figured out what steps will work) should be to try to write so that someone else in this class would be able to easily follow, understand and believe the steps. Your proof must include justification (generally what previous theorem or homework problem allows you to make a particular statement or conclusion), and should include enough detail so that no one has to guess what it is your proof is a proof for. Best way to accomplish the latter is to simply make the first sentence (or first few sentences) tell the reader what you are assuming to be true, then end with "Therefore, (whatever the conclusion is supposed to be)." When in doubt, put in more steps rather than fewer. If your proof is "correct", I won't count off if you have written more than is enough to do the proof (unless some of the extra stuff is wrong or not related). Also if the proof involves showing one thing is equal to another, it is always bad (and sometimes dangerous) to put in the equation until you actually have it established. We aren't solving equations, we are proving things. **Start with one side and work your way through until you have what you were asked to prove.** Frequently, it is good idea to do a little "scratch work" before writing your proof. You can take a little bit more liberty here, but keep in mind that you want to start with what is on one side, and transform it into the other. There is no need to include the scratch work in what you turn in for homework.

****

We won't be doing proofs like the below until late February.

Here is the basic scheme for proving a set X is a "subring" of some given ring Y.

Generally the set X will be given in the form $X = \{s \in Y \mid s$ "does something special"$\}$ where "does something special" will vary from problem to problem–**don't look back and try to use the same "does something special" from a previous problem**. You have to use what "does something special" is for the particular problem you are working on.

The conclusion will always have the form "Therefore X is subring of Y by the Subring Theorem." where X is the name of the set you are supposed to prove is a subring of the ring whose name is Y.

Step 1: Show the zero element of the ring Y satisfies the "does something special" for the set X. Generally this will require a theorem. Possibilities for which particular theorem is needed include the "Ring Theorem" and the "Homomorphism Theorem". The zero element of the ring Y is usually written as 0_Y, unless we know more about the ring Y. For example the zero element of the ring $\mathbb{Z}_n$ is written as $[0]$. Once you have established that the zero element of the ring Y satisfies the "does something special", then the next sentence would be, "Thus 0_Y is in X." or the condensed version "Thus $0_Y \in X$."

Step 2: Next pick two letters to represent a pair of elements of the set X. The sentence should simply say "Let $b, c \in X$." or "Let b and c be elements of X." **DO NOT SAY ANYTHING ELSE IN THIS SENTENCE–YOU WILL BE PENALIZED IF YOU DO.** To be safe, do not use letters that appear anywhere in the statement of the problem because there will be problems where the "does something special" involves some particular fixed element of the ring Y. For example, if the problem says the letter t is a fixed element of Y, then you cannot use t to represent an element of X (and with regard to the warning in Step 3, you cannot use it for the "for some ...").

Step 3: The sentence after "Let $b, c \in X$" should be where you say that b and c satisfy the "does something special" condition. Usually some kind of equation will be part of the "does something special". If so, put b and c in the same place as the letter on the **left side** of the "|" in the description of the set $X = \{s \in Y \mid s$ "does something special"$\}$, and include any phrase that might be included in the "does something special" – in this example b and c would go where the "s" is on the **right side** of the "|". Warning: if the "does something special" includes a "for some ....", you must use different letters for the "for some ...", one for each of b and c.

Step 4: The actual "proof part" is what comes next. You have to show $b + c$, $-b$ and bc are also in the set X by showing they also satisfy the "does something special". What you do here varies from problem to problem. Frequently the sum will use the distributive property of multiplication over addition–but sometimes it does not. Almost always you will need a theorem to get $-b$ to satisfy the "does something special". The two that will be used most often are the "Ring Theorem" and the "Homomorphism Theorem." Sometimes you will need a theorem ("Ring Theorem" or "Homomorphism Theorem") to show the product bc satisfies the "does something special", but sometimes the only thing you need is the associative property of multiplication. You must say that all three of $b + c$, $-b$ and bc are in the set X after showing that each satisfies the "does something special".

Step 5: Finally end with "Therefore X is a subring of Y by the Subring Theorem."

Special Markings

(1) On occasion I will make a mark on your paper and write "OK to here". If you have one of these, then the next statement is either false or lacking something that is very important. **It also means that there is a way to continue from that point and end up with a correct and well-written proof. Before abandoning your approach, try to complete the proof from this point. If you go back farther, you run the risk of ending up with a lower score on your revision than on your original.**

(2) If you see the word "Why", you need to provide some reference as to why that particular statement can be made at this point in your proof. Generally either some theorem or previous homework problem, but sometimes based on a special property – like "...since T is a subring of R., or "...since f is a homomorphism." There is nothing wrong at that point other than failure to justify the statement. You do not need to justify use of terms like "divides" or "is congruent to", but a few terms (like "homomorphism") will require justification. Follow the pattern used in the proofs I do in class with regard to definitions. Standard deduction for "Why" is one point.

(3) "Not the reason" or "Not by Fill In The Blank Theorem" or "Wrong reason" or "Wrong Theorem" means whatever reason/justification you used is not correct–possibly because the conclusion of the "wrong theorem" has nothing to do with what you want to conclude (for example, the Divisor Theorem is only good for proving something like $a \leq b$, it is almost never the reason one integer divides another), or maybe because you haven't shown what you need to apply the theorem (for example, if you are asked to prove d is the gcd of integers r and s, you can't say "d divides both r and s by the GCD Theorem"–instead you have to prove d divides both r and s **AND at least two more things** before you can conclude: "Therefore $d = gcd(r, s)$ by the GCD Theorem.").

(4) The comment "What is this (are these)?" means you have introduced a new letter(s) in the proof and need to say what that letter represents.

(5) The comment "Big Gap" means you have left out some necessary steps ("Gap" means one step missing). "Huge Gap" means you have left out way too many steps.

(6) The comments "Very wrong" and "Very, very wrong" mean what you have written is, as you might suspect, either very wrong or very, very wrong.

(7) The comment "Can't assume this" more than likely means you have declared something to have a special value when you are not allowed to make such a claim. To avoid getting this comment, (i) never ever make a letter do more than one thing, and (ii) if a particular letter is given in the statement of the problem, don't declare that it does some specific thing in your proof, all you can hope for is that you will be able to show why it does some specific thing if that is (part of) what you are asked to prove.

(8) The comment "Conclusion?" means you haven't finished the proof yet. More than likely, it simply means you haven't written down the conclusion given in the problem. Standard deduction is one point if that is all that is missing–but make sure you put in a reason when you do the revision to avoid getting "Why?" the second time around. A related comment is "So?". If "So?" appears at the end, it means you are missing a little more that just the conclusion. If "So?" appears in the middle, it generally means you have done some useful step but didn't say what good that step does. [For some problems, your conclusion should match the conclusion of the problem exactly – like in the first two examples of proofs – but in others it may be slightly different – like the last proof about integer solutions.]

(9) The comment "What are you assuming?" means you left out what you are assuming to be true at the beginning of the proof. Write your proof so you don't need to look at the problem to see exactly what it is you are proving.

(10) The comment "Not what was given" means you have not started with what you were supposed to start with. Use exactly what is given in the problem, not a consequence of what is given.

(11) The comment "Symbol not allowed" means you have used one of the forbidden symbols.

(12) The comment "No ab." means you are not allowed to abbreviate words. Write the entire word.

(13) The comment "Wrong order" means you have a string of equations where some or all of the equations directly connect two things that you cannot claim are directly equal. For example it is perfectly okay to write either $ad = a(b+c) = ab+ac$ or $ab+ac = a(b+c) = ad$ if you know $d = b+c$, but not okay to write $a(b+c) = ad = ab+ac$.