115A HWK 1 Selected Solutions

Sam Qunell

January 19, 2023

Below are my solutions to a few of the problems on the first homework assignment. I generally choose problems that I think demonstrate many of the concepts we have discussed and that I know many students wanted to see.

My writing style here is probably more technical and pedantic than what is actually *required* for you, and perhaps even more than what is *expected* of an actual mathematician. My style will also be somewhat repetitive because I want each portion of the proof to be self-contained. In general mathematics, one may casually avoid this repetition by saying things like "similarly to the work above, such and such is true". I think it is still useful as an instructive tool for one to be able to see all of the different considerations that go into organizing a complete proof.

In each problem, I will include some remarks about things that you should be thinking about in approaching such a problem, areas where many students tend to go wrong, and the general utility of the theorem in the problem. These things do not actually need to be included in a proof and are just my commentary.

I want to emphasize that there may be multiple ways to solve certain problems. Even if your solution looks very different from mine, it may still be valid.

Problem 4

Consider the subset of $\mathbb{C}$: $\mathbb{Q}(i) = \{x + yi : x, y \in \mathbb{Q}\}$. Prove that $\mathbb{Q}(i)$ with the addition and multiplication inherited from $\mathbb{C}$ is a field.

Proof. We first check that $\mathbb{Q}(i)$ is closed under addition and multiplication, i.e., the given addition and multiplication are indeed binary operations on this set. Let $x + yi$ and $a + bi$ be two $\mathbb{Q}(i)$ elements for $x, y, a, b \in \mathbb{Q}$. Via commutativity and associativity of addition in $\mathbb{C}$, we have that $(x + yi) + (a + bi) = (x + a) + (y + b)i$. Since $x, a, y, b \in \mathbb{Q}$, which is a field, so are the sums $x + a$ and $y + b$. So, our sum is in $\mathbb{Q}(i)$ by definition. Likewise, by the distributivity of $\mathbb{C}$, we compute that $(x+yi)*(a+bi) = xa+yia+xbi+yibi$. By associativity of addition, and commutativity of addition and multiplication in $\mathbb{C}$, this is $xa+ybi^2+yai+xbi = (xa - yb) + (ya + xb)i$. Since $x, a, y, b \in \mathbb{Q}$, so are the terms $xa - yb$ and $ya + xb$. So, this is also in $\mathbb{Q}(i)$ by definition. So, the addition and multiplication of $\mathbb{Q}(i)$ are indeed binary operations. We now verify each of the field axioms. Fix $a + bi, x + yi, c + di \in \mathbb{Q}(i)$ with $x, y, a, b, c, d \in \mathbb{Q}$.

1. We check commutativity of addition. Consider the sum $(a + bi) + (x + yi)$. Since the addition on $\mathbb{C}$ is equal to the addition on $\mathbb{Q}(i)$, and since $F1$ holds for the field $\mathbb{C}$, this is equal to $(x + yi) + (a + bi)$ as desired.

   To check commutativity of multiplication, consider the product $(a+bi)*(x+yi)$. Since the multiplication on $\mathbb{C}$ is equal to the multiplication on $\mathbb{Q}(i)$ and since $F1$ holds for the field $\mathbb{C}$, this is equal to $(x + yi) * (a + bi)$.

2. We check associativity of addition. Consider the sum $(a + bi) + ((x + yi) + (c + di))$. Since the addition on $\mathbb{C}$ is equal to the addition on $\mathbb{Q}(i)$, and since $F2$ holds for the field $\mathbb{C}$, this is equal to $((a + bi) + (x + yi)) + (c + di)$.

To check associativity of multiplication, consider the product $(a+bi)*((x+yi)*(c+di))$. since the multiplication on $\mathbb{C}$ is equal to the multiplication on $\mathbb{Q}(i)$, and since $F2$ holds for the field $\mathbb{C}$, this is equal to $((a+bi)*(x+yi))*(c+di)$.

3. We show existence of additive identity. Note $0 \in \mathbb{Q}$. Consider $0+0i \in \mathbb{Q}(i)$. Then by the field axioms in $\mathbb{C}$, $(a+bi)+(0+0i) = (a+0)+(b+0)i = a+bi$. So, $0+0i$ is indeed the additive identity.

   To show existence of multiplicative identity, note $1 \in \mathbb{Q}$. We will show $1+0i$ is this multiplicative identity. By field axioms in $\mathbb{C}$, we see $(a+bi)*(1+0i) = (a*1-b*0)+(a*0+b*1)i = a+bi$, as desired.

4. We show existence of additive inverse. Note that $-a$ and $-b \in \mathbb{Q}$ since a and b are. So, $-a+(-b)i \in \mathbb{Q}(i)$. By field axioms in $\mathbb{C}$, we compute $(a+bi)+(-a+-bi) = (a+-a)+(b+-b)i = 0+0i$. So, $-a+(-b)i$ is the additive inverse of $a+bi$.

   We now show existence of multiplicative inverse. Note that if $a+bi \neq 0$, then either a is nonzero or b is nonzero. In either case, $a^2+b^2 \in \mathbb{Q}$ and is nonzero. Since $\mathbb{Q}$ is a field, we see that $\frac{a}{a^2+b^2}$ and $\frac{-b}{a^2+a^2}$ are both well-defined and are in $\mathbb{Q}$. We will show that $\frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2} \in \mathbb{Q}(i)$ is the multiplicative inverse of $a+bi$. We compute from the $\mathbb{C}$ field axioms that $(a+bi)(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i) = \frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2} + \frac{abi}{a^2+b^2} + \frac{-abi}{a^2+b^2} = \frac{a^2+b^2}{a^2+b^2} + \frac{abi-abi}{xa^2+b^2} = 1+0 = 1$. So, $\frac{a}{a^2+b^2} + \frac{-bi}{a^2+b^2}$ is indeed the multiplicative inverse of $a+bi$.

5. We show distributivity. Consider the expression $(a+bi)*((x+yi)+(c+di))$. Since the addition and multiplication in $\mathbb{Q}(i)$ are the same as those in $\mathbb{C}$, and since $\mathbb{C}$ satisfies the distributivity axiom, this expression equals $(a+bi)*(x+yi)+(a+bi)*(c+di)$.

So, $\mathbb{Q}(i)$ satisfies all field axioms and is thus a field by definition. □

Several students verified some of these axioms by directly computing expressions like $a+(b+c)$ in $\mathbb{C}$. This is valid as long as you state you are using rules in $\mathbb{C}$. You want to be careful to not use commutativity in $\mathbb{Q}(i)$ before you have proven it exists.

My solution here appeals often to the nice field axioms in $\mathbb{C}$ to avoid these kinds of circular reasoning issues. I think for this problem, spelling out precisely which axioms in what order is not really essential (although some may disagree).

If you are observant, you may notice that these redundant appeals to $\mathbb{C}$ rules can actually be cut out entirely if you use problem 5 to prove this one. As I demonstrate, $\mathbb{Q}(i)$ is a subset of a larger field that is closed under addition, multiplication, inverses, and contains the identities. So, problem 5 guarantees that $\mathbb{Q}(i)$ is a field with the inherited operations. As long as you explain this clearly and check the conditions that you need to check, this should also be valid.

One common source of error is in proving that the nonzero $a+bi$ has a multiplicative inverse. Some students write things like "$\frac{1}{a+bi}$ exists because nonzero complex numbers have multiplicative inverses". This is a true statement, but unfortunately not what you are attempting to demonstrate. In order for $\mathbb{Q}(i)$ to be a field, it needs to contain multiplicative inverses for each of its nonzero elements. So, while we know $\frac{1}{a+bi}$ is a perfectly good complex number, *one still needs to prove that it is contained in* $\mathbb{Q}(i)$. From these first principles, the only way to demonstrate that a given complex number is contained in $\mathbb{Q}(i)$ is from the definition of this set. To show that $\frac{1}{x+yi} \in \mathbb{Q}(i)$, you need to find $a', b' \in \mathbb{Q}$ such that $(a+bi)*(a'+b'i) = 1$.

For similar reasons, you do need to verify that this set $\mathbb{Q}(i)$ is closed under addition and multiplication. A field by definition has two *binary operations* on it, addition and multiplication. A binary operation takes two elements of that set as arguments and returns another element of that set. So, for example, if $a+b \notin \mathbb{Q}(i)$ even though a and $b \in \mathbb{Q}(i)$, then $+$ isn't a binary operation at all. It doesn't make much sense to talk about the commutativity of the binary operation $+$ and to evaluate expressions like $a+b$ if we don't even know $a+b$ is in our set!.

More concretely, consider the set $\{-1,0,1\} \in \mathbb{Q}$. This set has additive inverses, multiplicative inverses for nonzero elements, and identities for both operations. However, this set *is not a field because it is not closed under addition and multiplication.* $1+1 \notin \{-1,0,1\}$. Even though the operations $+$ and $*$ used are

those of $\mathbb{Q}$, which we know has all of our nice axioms, we should not have to think about larger sets when we deal with abstract objects.

The blue text (Via) is my way of telling the reader which mathematical facts/properties are justifying the conclusions that I draw. In many cases, there will be facts that seem obvious or straightforward to you, but much less so to whomever reads your proof. In other cases, your proof will be wrong because you needed stronger justification than you really had in order to use the result you want. Both problems can be avoided by carefully spelling out how you are making deductions.

The blue text (with) is my reminder to you that whenever you write down *any* variables or set elements, you should always specify what set they are a member of. A big piece of this problem is noting why certain elements exist in $\mathbb{Q}(i)$ at all, and this follows from the closure rules that we know about $\mathbb{Q}$.

Problem 6

Let $(F, +, *)$ be a field.

- Prove that $-1 * a = -a$ for any a in F.
- Prove that $-2 * a = -(2a)$ for any $a \in F$.
- Prove that for any nonzero $a \in F$, $(-a)^{-1} = -(a^{-1})$.

Proof.

- Fix $a \in F$. By uniqueness of the additive inverse in F, we know that if $-1 * a + a = 0$ then $-1 * a$ is exactly the additive inverse $-a$. So, we show that $-1 * a + a = 0$. By axiom F3, we may write the left hand side as $-1 * a + a = -1 * a + 1 * a$. By axiom F5, this is $(-1 + 1) * a$. By axiom F4, this is $0 * a$. By a result from class, this is 0. So indeed, $-1 * a$ is the additive inverse of a, i.e. $-1 * a = -a$.
- Fix $a \in F$. By uniqueness of the additive inverse in F, we know that if $-2 * a + 2 * a = 0$ then $-2 * a$ is exactly the additive inverse $-(2 * a)$. So, we show that $-2 * a + 2 * a = 0$. By axiom F5, we may write $-2 * a + 2 * a = (-2 + 2) * a$. By axiom F4, this is $0 * a$. By a result from class, this is 0. So indeed, $-2 * a$ is the additive inverse of $2a$, i.e. $-2 * a = -(2 * a)$.
- Fix $a \in F$ such that $a \neq 0$. By uniqueness of the multiplicative inverse in F, we know that if $-(a^{-1}) * -a = 1$ then $-(a^{-1})$ is exactly the multiplicative inverse $(-a)^{-1}$. So, we show that $-(a^{-1}) * -a = 1$. By the first part of this problem, we rewrite the left hand side as $-(a^{-1}) * -a = (-1 * a^{-1}) * (-1 * a)$. By commutativity and associativity of multiplication in F, this equals $(-1 * -1) * (a^{-1} * a)$. By axiom F4, this is $(-1 * -1) * 1$. By $F3$, this is $-1 * -1$. By the first part of the problem, this is $-(-1)$. Since $1 + -1 = 0$ by F4, we have that 1 is the additive inverse of -1, and so $-(-1) = 1$. So indeed, $-(a^{-1})$ is the multiplicative inverse of $-a$, i.e. $-(a^{-1}) = (-a)^{-1}$.

□

The statements in the problem may have looked "obvious" to you, but the elements $-1 * a$ and $-a$ are defined in different ways to satisfy different conditions. This problem is here to make sure you know what $-a$ really is, and that you are comfortable enough with the field axioms to use them in proofs.

If you are still getting used to this kind of axiomatic thinking, then you may have had trouble figuring out *which* axioms to use in order to show the desired equality. For this, I want to say that there isn't necessarily a single way of using these axioms. Oftentimes, the equation you have before you just reminds you of an expression appearing in one of the axioms, in the same way that $-1 * a + a$ almost looks like part of the distributivity axiom. There may be a few failed attempts on your first try, but ultimately you are going to want to think about which axioms look the most like what expression you currently have.

The blue text (Fix) means that, even though a can be *any* element of F, we are not going to fiddle with it after I have written it down. The idea is that if I pick any a at random, then the property holds for that single a. The a here was indeed "drawn at random". The point is that you want to avoid situations where you treat a like a variable input to a function. a here must always have a *single* value at a time. The

argument is that this single value is irrelevant to the proposition. In practice, this is more of a stylistic issue, but you do want to promise your reader that you are not varying things that are not actually variable.

The blue text (So, we show that) is indicating that I am about to prove a "secondary" statement that will imply the claim I want. This is justified as long as you explain why the primary statement follows from the secondary statement. You could also reorganize the proof to avoid this if you like. One could first show that $-1 * a + a = 0$, and *then* say something like "because additive inverses are unique in F, this means that the listed element is indeed the additive inverse". As long as you make clear why the computations that you write are demonstrating the result you want, you should be fine.

The blue text (So indeed) is another stylistic feature. Formally, one does not need to repeat the claim if you have already stated somewhere what you are going to prove. It is good general practice. A common saying in math writing (or any writing) is that you should always make your argument three times. First, you tell the reader what you are going to do. Then, you do it. Then, at the end, you remind the reader what you just did. It sounds silly, but I think it can be a good practice to get you into the habit of thinking mathematically.

The blue text (By the first part of this problem) may have surprised you if you did not realize this was allowed. You do not have to re-prove the first part in the third part *as long as you are clear why you know the equality holds.*