Math 371, Spring 2013, PSet 1

Aaron Michael Silberstein

January 10, 2013

This problem set will be due Friday, January 18, 2013 at 1 pm in Matti's mailbox.

1 The Craft (and Art) of Writing Proofs

Writing proofs and producing mathematics, like any other creative endeavor, has two components: an art, and a craft. The *art* is the act of creation, an internal process which stems from experience and inspiration; the craft is the mastery of the skills which must are routinely employed in effecting the art. While we do math for ourselves, we write proofs for others. **We perfect our craft so others may benefit from our creativity.**

These problem sets will hopefully help you improve your mathematics, in both art and craft. Since many of you are relatively inexperienced proof writers (with the capacity to produce great proofs, I think!) we will focus at the beginning mostly on the craft of proof writing.

One needs, at the beginning of one's mathematical education, to learn how to write what I call *routine proofs*. These are proofs of facts that are fairly close to the definitions — where the idea of the proof is relatively simple, and the most important thing is to express this simple idea clearly and precisely.

The first thing to remember when writing proofs is that a proof is a sequence of true statements from which one eventually deduces a statement (the theorem), ideally without extraneous argument. This process is painstaking and tedious at first; much of what I write below might seem overly pedantic. I believe, however, that it is important to realize how much goes into a relatively compact theorem/proof; and so I will try to guide you through this process as completely as possible, just this once.

Let's try to prove:

Theorem 1. *Let $f : G \to H$ and $f' : H \to I$ be injective group homomorphisms. Then $f' \circ f : G \to I$ is an injective group homomorphism.*

The first step in any such proof is breaking the theorem into hypotheses and conclusions. We want to do this in such a way that we can use basic set theory and logical deduction to write our proof.

The hypotheses are:

1. $(G, \cdot, e), (H, \cdot, e)$ and $(I, \cdot, e)$ are groups. Notice that this is implicit in the statement of the theorem, and not explicit; only G, H, and I are given as symbols. But in order for f and g to be group homomorphisms, G, H, and I have to have group structures. We use the convention that multiplication on all groups is denoted by the same $\cdot$, and that the identity is denoted by e. However, we must be careful to understand when this leads to ambiguity and when this doesn't. For instance, in the expression $f(g) \cdot e$, $\cdot$ and e only make sense if they are in H, because $f(g)$ must be in H (and g must be in G) and we cannot multiply group elements in different groups together. However, if I say $\cdot$ is commutative, I had better specify in which group!

2. f and f' are injective as maps of sets. That is, for all $g, g' \in G$, if $f(g) = f(g')$ then $g = g'$; and for all $h, h' \in H$, if $f'(h) = f'(h')$ then $h = h'$.

3. f and f' are group homomorphisms:

   (a) For all $g, g' \in G$, $f(g \cdot g') = f(g) \cdot f(g')$; and for all $h, h' \in H$, $f'(h \cdot h') = f(h) \cdot f(h')$.

   (b) $f(e) = e$ and $f'(e) = e$.

Problem 1. *We just wrote "$f(e) = e$ and $f'(e) = e$." Rename all the e's as e_1, e_2, e_3 and e_4 respectively so we have $f(e_1) = e_2$ and $f'(e_3) = e_4$. To which sets (out of G, H, and I) do each of the e_i's belong? How do you know?*

Now, we need to write down the conclusions we seek:

1. $f' \circ f$ is injective. For all $g, g' \in G$, if $f'(f(g)) = f'(f(g'))$ then $g = g'$.

2. $f' \circ f$ is a group homomorphism. For all $g, g' \in G$, $f'(f(g \cdot g')) = f'(f(g)) \cdot f'(f(g'))$ and $f'(f(e)) = e$.

You must check that $f' \circ f$ is well-defined. To write the proof, we now need to write down statements starting from the hypotheses which lead to the conclusion. Let's tackle the first statement: For all $g, g' \in G$, if $f'(f(g)) = f'(f(g'))$ then $g = g'$. To prove this, we will need to start with a statement which allows us to say something about all $g, g' \in G$. I see two:

1. For all $g, g' \in G$, if $f(g) = f(g')$ then $g = g'$.

2. For all $g, g' \in G$, $f(g \cdot g') = f(g) \cdot f(g')$.

Only one of these deals with functions taking as inputs only g and g' separately, so we can guess that we should start to write down that statement first (and justify!):

Proof. f is injective, so for all $g, g' \in G$, if $f(g) = f(g')$ then $g = g' \ldots$ □

So that's a good start. Now, we look at the conclusion: something involving "if $f'(f(g)) = f'(f(g'))\ldots$". Similarly, we see that there is one statement which reduces to a statement involving $f'(-) = f'(-)$: for all $h, h' \in H$, if $f'(h) = f'(h')$ then $h = h'$. But now, we already have our h and h': $f(g)$ and $f(g')$! We now can use logic: if we know "for all X, then Y(X)", then we know Y(X) is true, for some instantiation of X. We may now write the next line of our proof:

Proof. f is injective, so for all $g, g' \in G$, if $f(g) = f(g')$ then $g = g'$. But f' is also injective, so if $f'(f(g)) = f'(f(g'))$ then $f(g) = f(g')$. Thus, if $f'(f(g)) = f'(f(g''))$ then $g = g'$, so $f' \circ f$ is injective.... □

Problem 2. *Prove, in the same way, that $f' \circ f$ is a group homomorphism. Put this together with the proof written immediately above to provide a full proof of the theorem.*

Problem 3. *Use the same method to prove the following theorems:*

1. *Let G be a group and N and M normal subgroups of G. Then $N \cap M$ is also normal.*
2. *Let R be a (not necessarily commutative) ring, and I and J left-ideals of R. Then $I \cap J$ is an ideal of R.*
3. *Let $f : V \to W$ and $f' : W \to X$ be surjective vector space homomorphisms. Then $f' \circ f$ is a surjective vector space homomorphism.*

2 A Blast From the Past

For these problems, you will need the structure theory of $k[t]$ as developed in class (in particular, some of the things I ask of you are restatements of things we have gone over in class). Let K be a field, and let the characteristic of K not be 2; that is, $1 + 1 \neq 0$ in K. Let now $f(t)$ be an irreducible, monic polynomial of degree 2; that is, $f(t) = t^2 + bt + c$ for some $b, c \in K, a \neq 0$.

Problem 4. *Prove that $K_f := K[t]/f(t)$ is a field.*

Problem 5. *Consider $f(t)$ as an element of $K_f[t]$. Prove that there exist $\gamma, \delta \in K_f$ such that $f(t) = (t - \gamma)(t - \delta)$. Prove that $\gamma \neq \delta$.*

We define $\mathrm{End}(K_f/K)$ *to be the set of field homomorphisms*

$$\sigma : K_f \to K_f$$

such that for any $k \in K$

$$\sigma(k) = k.$$

Prove that $\mathrm{End}(K_f/K)$ *is a group with the group law given by composition. Thus,* $\mathrm{End}(K_f/K)$*, the set of endomorphisms of K_f/K is equal to* $\mathrm{Aut}(K_f/K)$*, the group of* ***automorphisms of*** *K_f/K.*

Problem 6. *Prove that an element of* $\mathrm{Aut}(K_f/K)$ *fixes a root of* f *if and only if it is the identity automorphism.*

Problem 7. *Conclude that* $\mathrm{Aut}(K_f/K)$ *has precisely two elements. The nontrivial element transposes the roots of* f*. Call the nontrivial element* σ*.*

Problem 8. *Prove that* $\sigma k = k$ *if and only if* $k \in K$*. Thus,* $\alpha \cdot \sigma\alpha \in K$ *and* $\alpha + \sigma\alpha \in K$ *for all* $\alpha \in K_f$*.*

Problem 9. *Let* $\phi(t) \in K[t]$ *be a quadratic polynomial such that* $\phi(t)$ *is irreducible in* $K[t]$ *but has a root in* K_f*. Prove that if* $\phi(a) = 0$ *then* $\phi(\sigma a) = 0$ *so*

$$\phi(t) = (t - a)(t - \sigma a).$$

Problem 10. *Let* $k \in K$ *be such that* $\phi(t) = t^2 - k$ *is irreducible over* K*. Prove that if* $\alpha \in K_f$ *is such that* $\phi(\alpha) = 0$ *then* $\phi(-\alpha) = 0$ *so* $\sigma\alpha = -\alpha$*. Conversely, if* $\sigma\alpha = -\alpha$*, prove that* $\alpha^2 \in K$ *but* $\alpha \notin K$*.*

Problem 11. *Show that* $\sigma(\gamma - \delta) = -(\gamma - \delta)$*. Conclude that* $(\gamma - \delta)^2 \in K$*.*

Problem 12. *Write* $(\gamma - \delta)^2$ *in terms of the coefficients* b *and* c*. Why can you do this? Call this number* Δ*, the* ***discriminant*** *of* f*. We now write* $\gamma - \delta = \sqrt{\Delta}$*.*

Problem 13. *Since* $b = -(\gamma + \delta)$*, conclude that*

$$\gamma = \frac{-b + \sqrt{\Delta}}{2}, \delta = \frac{-b - \sqrt{\Delta}}{2}.$$

This is the quadratic formula.