Intro to Math Reasoning HW 11b

Ozaner Hansha

December 12, 2018

Problem 1

Part a

Problem: Prove that the additive inverses of every element in a field are unique:

$$(\forall x \in F)\, x + a = 0_F \wedge x + b = 0_F \to a = b$$

Solution: Consider the following chain of equalities:

$$\begin{aligned}
a &= a + 0_F && \text{(additive identity)}\\
&= a + (x + b) && \text{(given)}\\
&= (a + x) + b && \text{(associativity +)}\\
&= (x + a) + b && \text{(commutativity +)}\\
&= 0_F + b && \text{(given)}\\
&= b && \text{(additive identity)}
\end{aligned}$$

Part b

Problem: Prove that the multiplicative inverses of every element in a field are unique:

$$(\forall x \in F)\, x \cdot c = 1_F \wedge x \cdot d = 1_F \to a = b$$

Solution: Consider the following chain of equalities:

$$\begin{aligned}
c &= c \cdot 1_F && \text{(multiplicative identity)}\\
&= c \cdot (x \cdot d) && \text{(given)}\\
&= (c \cdot x) \cdot d && \text{(associativity $\cdot$)}\\
&= (x \cdot c) \cdot d && \text{(commutativity $\cdot$)}\\
&= 1_F \cdot d && \text{(given)}\\
&= d && \text{(multiplicative identity)}
\end{aligned}$$

Problem 2

Part a

Problem: Prove that the additive identity 0_F in a field is an absorbing element under multiplication:

$$(\forall x \in F)\, x \cdot 0_F = 0_F$$

Solution: First note the following:

$$\begin{aligned} x \cdot 0_F &= x \cdot (0_F + 0_F) && \text{(additive identity)} \\ &= x \cdot 0_F + x \cdot 0_F && \text{(distributive property)} \end{aligned}$$

Now we can see that:

$$\begin{aligned} x \cdot 0_F &= x \cdot 0_F + x \cdot 0_F \\ x \cdot 0_F + (-x \cdot 0_F) &= x \cdot 0_F + x \cdot 0_F + (-x \cdot 0_F) && \text{(additive inverse exists)} \\ 0_F &= (x \cdot 0_F + x \cdot 0_F) + (-x \cdot 0_F) && \text{(additive inverse)} \\ 0_F &= x \cdot 0_F + (x \cdot 0_F + (-x \cdot 0_F)) && \text{(associativity)} \\ 0_F &= x \cdot 0_F + 0_F && \text{(additive inverse)} \\ 0_F &= x \cdot 0_F && \text{(additive identity)} \end{aligned}$$

Part b

Problem: Prove the following:

$$(\forall x, y \in F)\, x \cdot y = 0_F \to x = 0_F \wedge y = 0_F$$

Solution: W.l.o.g we can split this proof into two cases, one where $x = 0_F$, and one where $x \neq 0_F$. These two cases exhaust the elements of the field. The first case is an immediate consequence of Part a:

$$x = 0 \to xy = 0$$

Now we consider the case where $x \neq 0$.

$$\begin{aligned} xy &= 0 \\ x^{-}1(xy) &= (x^{-}1)0 && \text{(nonzero elements have multiplicative inverse)} \\ (x^{-}1x)y &= (x^{-}1)0 && \text{(associativity of multiplication)} \\ (1_F)y &= (x^{-}1)0 && \text{(multiplicative inverse)} \\ (1_F)y &= (x^{-}1)0 && \text{(multiplicative identity)} \\ y &= (x^{-}1)0 && \text{(multiplicative identity)} \\ y &= 0 && \text{(part a)} \end{aligned}$$

And we are done. We showed that either $x = 0_F$ or, if not, $y = 0_F$. Note that this does not preclude them both being 0_F.

Problem 3

Problem: Prove that for any prime p, every element in $\mathbb{Z}_p$ has a multiplicative inverse.

Solution: We can phrase this as:

$$(\forall n \in \mathbb{Z}_p)\, n \neq 0 \rightarrow (m \in \mathbb{Z}_p)\, mn = 1$$

So let us assume the antecedent and derive the consequent. Note that since p is prime and because we are assuming $n \neq 0$ the following is true:

$$\mathrm{gcd(n, p)} = 1$$

This is because p is prime and n cannot divide it. We know that GCD's have the following property for some $a, b \in \mathbb{Z}$:

$$1 = \mathrm{gcd(n, p)} = an + bp$$

Now let us evaluate this equation in mod p:

$$[1]_p = [an + bp]_p = [an]_p + = [bp]_p = [a]_p[n]_p + [b]_p[p]_p$$

Now note that $[p]_p = [0]_p$ leaving us with:

$$[1]_p = [a]_p[n]_p$$

And we are done. We have constructed an inverse of n, namely a.

Problem 4

Problem: Define $f : \mathbb{Z}_{\leq 1} \rightarrow F$ recursively as follows: $f(1) = 1_F$, and for $n \leq 2$, $f(n) = f(n-1) + 1_F$. Prove that f is injective. Deduce that F must be infinite.

Solution: Proving the injectivity of f means proving:

$$(\forall a, b \in \mathbb{Z}_{\leq 1})\, f(a) = f(b) \rightarrow a = b$$

First let us consider the following notation:

$$\underbrace{1_F + 1_F + \cdots + 1_F}_{n} \equiv n_F$$

Now let us consider the following proposition:

$$P(n) \equiv n_F < n_F + 1_F$$

This is a consequence of $0_F < 1_F$ and the order field axiom:

$$a < b \to a + 1_F < b + 1_f$$

using induction on these two it's clear that $P(n)$ holds for all $\mathbb{Z}_{\leq 1}$.

Now since the function $f(n)$ is increasing with every iteration, we know that only $f(1) = 1_F$ because $f(1+n) = (1+n)_F$ for $n > 1$. We can make the same argument inductively for all integers above 1 meaning our function is one-to-one.

Problem 5

Problem: Consider the set of real numbers of the form $p+q\sqrt{2}$ where $p, q \in \mathbb{Q}$. Prove that this is closed under addition and multiplication and contains multiplicative and additive inverses for every element.

Solution: It is closed under addition:

$$\begin{aligned}
&(p + q\sqrt{2}) + (r + s\sqrt{2}) \\
&= (p + r) + (q\sqrt{2} + s\sqrt{2}) && \text{(commutativity/associativity)} \\
&= (p + r) + (q + s)\sqrt{2} && \text{(distributivity)}
\end{aligned}$$

Note that the rationals are closed under addition (we can always put two fractions in terms of a common denominator then add), and so $(p+r)$ and $(q+s)$ are rationals. Thus addition is closed.

Now for multiplication:

$$\begin{aligned}
&(p + q\sqrt{2})(r + s\sqrt{2}) \\
&= pr + ps\sqrt{2} + qr\sqrt{2} + 2qs && \text{(foil (distributivity))} \\
&= (pr + 2qs) + ps\sqrt{2} + qr\sqrt{2} && \text{(commutativity/associativity)} \\
&= (pr + 2qs) + (ps + qr)\sqrt{2} && \text{(distributivity)}
\end{aligned}$$

Due to the closure of rationals under multiplication (multiply numerators then denominators) and addition, $(pr + 2qs)$ and $(ps + qr)$ are rationals and so multiplication is closed.

Now for inverse additive elements:

$$-(p + q\sqrt{2}) = -p - q\sqrt{2}$$

Because multiplication is closed under the rationals, we can multiply our element by -1 to arrive at the inverse which is also in the field.

Finally, the multiplicative inverses:

$$\begin{aligned}
\frac{1}{p+q\sqrt{2}} &= \frac{1}{p+q\sqrt{2}} \cdot \frac{p-q\sqrt{2}}{p-q\sqrt{2}} \\
&= \frac{p-q\sqrt{2}}{p^2-2q^2} \\
&= \frac{p}{p^2-2q^2} + \frac{-q}{p^2-2q^2}\sqrt{2}
\end{aligned}$$

And since the rationals are closed under addition, subtraction, multiplication, and division $\frac{p}{p^2-2q^2}$ is a rational and so is $\frac{-q}{p^2-2q^2}$. Thus, all of the elements in our fields have multiplicative inverses in the field. This presupposes p and q are non-zero but if they were then the element of F they comprise would be 0 and thus not have an inverse regardless.