115AH Week 1 Tuesday Notes

January 14, 2021

1 HW 1 Problem 1

Let A and B be finite sets with the same number of elements. Let $f : A \to B$ be a function.

Show the following are equivalent:

(1) f is a bijection.

(2) f is an injection.

(3) f is a surjection.

1.1 $(1) \Rightarrow (2)$

By definition, bijections are injections.

1.2 $(2) \Rightarrow (3)$

We proceed by induction on the number of elements in A and B.

When $|A| = |B| = 1$, there is only 1 function from A to B and it is a surjection.

Now suppose the statement is true for sets of size less than $|A|$ and $|A| > 1$.

Let $f : A \to B$ be an injection. Choose $a \in A$ and define $f|_{A-\{a\}} : A - \{a\} \to B - \{f(a)\}$ by $f|_{A-\{a\}}(x) = f(x)$.

This is well defined as the only value such that $f(x) = f(a)$ is a.

Furthermore observe that $f|_{A-\{a\}}$ is injective.

Then by the induction hypothesis, $f|_{A-\{a\}}$ is surjective.
Hence $B - \{f(a)\} \subseteq \operatorname{Im} f$. As $a \in \operatorname{Im} f$, we see that $B \subset \operatorname{Im} f$. Hence f is surjective.

1.3 (3) $\Rightarrow$ (1)

Let $f : A \to B$ be surjective.

Define $g : B \to A$ as follows:
For $b \in B$, there exists some $a \in A$ such that $f(a) = b$. For each b choose one a such that $f(a) = b$ and set $g(a) = b$.

Observe that g is injective. Indeed, if $g(b) = g(b') = a \in A$ then $f(a) = b$ and $f(a) = b'$. Hence $b = b'$ so g is injective.

Then by the previous part, g is also surjective and hence a bijection. We claim that $f = g^{-1}$. In particular, let $h = g^{-1}$ and we will show that $f = h$.

We have that $h(g(b)) = b$ and $g(h(a)) = a$ for all $b \in B$ and $a \in A$.
Let $x \in A$. As g is surjective, there exists $y \in B$ such that $g(y) = x$.
Then $f(x) = f(g(y)) = y$ (by the construction of g) and $h(x) = h(g(y)) = y$.

Hence for all $x \in A, f(x) = h(x)$, so $f = h$.

Hence f has an inverse g and is hence a bijection.

2 Problem 3

Fields with 3, 4, and 5 elements.

The following addition and multiplication tables work:

2.1 3 elements

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2.2 4 elements

$+$	0	1	t	$1+t$
0	0	1	t	$1+t$
1	1	0	$1+t$	t
t	t	$1+t$	0	1
$1+t$	$1+t$	t	1	0

$\times$	0	1	t	$1+t$
0	0	0	0	0
1	0	1	t	$1+t$
t	0	t	$t+1$	1
$1+t$	0	$1+t$	1	t

Here we do polynomial multiplication with the rule $t^2 \equiv t+1$. Why this works is a question with a deep answer, but requires a great deal more math than we have developed.

2.3 5 elements

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2.4 No field with 6 elements.

As was shown in extra lecture 2, a finite field must have a prime power number of elements.

3 Problem 6

Let V be a vector space over F and W_i subspaces of V for all $i \in I$. Prove that $U = \bigcap_{i \in I} W_i$ is a subspace of V.

We use the subspace test.

First observe that as $\vec{0} \in W_i$ for all i, $\vec{0} \in U$ so U is non-empty.

Next let $u, v \in U$ and $\alpha \in F$. Then for all $i \in I, u, v \in W_i$. As W_i is a subspace, $u + \alpha v \in W_i$ as well.
Hence $u + \alpha v \in U$, so U is a subspace.