Mathematical Logic (MATH6/70132;P65)
Notes on Solutions to Problem Sheet 8

[0] Using AC, prove that if $f : C \to D$ is a surjective function, then there is an injective function $g : D \to C$ with $f(g(d)) = d$ for all $d \in D$. Does this statement imply AC (given the ZF axioms)?

Solution: Let h be a choice function for C (so, for every non-empty $Y \subseteq C$, we have $h(Y) \in Y$). The existence of this is given by AC. Define $g : D \to C$ by $g(d) = h(\{c \in C : f(c) = d\})$ for $d \in D$, noting that as f is surjective, the set $\{c \in C : f(c) = d\}$ is non-empty. It follows from the definition of g that $f(g(d)) = d$ for all $d \in D$, as required.

The given statement does imply AC. Suppose A is a set of non-empty sets. Let $B = \bigcup A$ and $C = \{(a, b) \in A \times B : b \in a \in A\}$. Define $f : C \to A$ by $f((a, b)) = a$ (for $(a, b) \in C$). This is surjective, so by the statement, there exists $g : A \to C$ with $g(f(a)) = a$ for all $a \in A$. Thus $g(a) = (a, b)$ for some $b \in a$. Let $h : C \to B$ be the map $h((a, b)) = b$. Then $k = h \circ g : A \to B$ is such that $k(a) \in a$ for all $a \in A$, as required.

Work in ZFC unless otherwise stated.

[1] (i) Suppose A is a set of cardinality λ and $\kappa \leq \lambda$ is a cardinal. Show that A has a subset B with $|B| = \kappa$.

(ii) Prove that ω is equinumerous with a proper subset of itself.

(iii) Suppose X is any set. Prove that X is infinite if and only if X is equinumerous with a proper subset of itself.
(Hint: use question 2, sheet 6 for one direction.)

Solution: (i) We have a bijection $f : \lambda \to A$. Note that $\kappa \subseteq \lambda$. Let B be $\{f(\gamma) : \gamma < \kappa\}$. Then f restricted to κ gives a bijection between κ and B and so B is a subset of A of cardinality κ.

(ii) Consider the map $f : \omega \to \omega$ given by $f(n) = n^\dagger$. This is injective but not surjective and ω is equinumerous with $\{n \in \omega : n > 0\}$.

(iii) First we show that no finite set is equinumerous with a proper subset of itself. It suffices to prove that for every $n \in \omega$, if $f : n \to n$ is injective, then f is surjective. This is done by induction on n. The case $n = 0$ is straightforward. Suppose we have the result for n and $g : n^\dagger \to n^\dagger$ is injective. By composing with a suitable bijection we may assume $g(n) = n$. Then g restricted to n is an injective function to n, so is surjective. Hence g is surjective.

Conversely, suppose X is an infinite set. So $|X| = \lambda \geq \omega$. By (i) there is a subset $Y \subseteq X$ with $|Y| = \omega$. By (ii) there is an injective function $f : Y \to Y$ which is not surjective. Now define $h : X \to X$ by $h(x) = f(x)$ if $x \in Y$ and $h(x) = x$ otherwise. This is injective, but not surjective, as required.

Remark: A set is said to be *Dedekind finite* if it is not equinumerous to a proper subset of itself. In ZFC we have just shown that this is the same as being finite (as defined on Problem sheet 7).

[2] (i) Suppose A, B, C are sets. Give a bijection between $A^{B\times C}$ and $(A^B)^C$.

(ii) Using the Fundamental Theorem of Cardinal Arithmetic, show that if A, B are sets with A infinite and $2 \leq |B| \leq |A|$, then $|B^A| = |\mathcal{P}(A)| = |2^A|$.
[Hint: Use the idea of Question 4(b) on Problem sheet 6.]

Solution: (i) Define a map $S : A^{B\times C} \to (A^B)^C$ as follows. Let $f : B \times C \to A$ be a function. Then $S(f) : C \to A^B$ sends $c \in C$ to the function $S(f)(c) : B \to A$ which maps b to $f(b, c)$ (so $S(f)(c)$ is the function $x \mapsto f(x, c)$ for $x \in B$). To show that S is bijective we can write down the inverse function $T : (A^B)^C \to A^{B\times C}$: if $h : C \to A^B$, let $T(h)(b, c) = h(c)(b)$.

(ii) We have a bijection from $\mathcal{P}(A)$ to 2^A which sends each $X \subseteq A$ to its characteristic function. So $|\mathcal{P}(A)| = |2^A|$.

We have injective functions $A \to A \times B$ and $A \times B \to A \times A$ (the latter using $|B| \leq |A|$). So using FTCA, $|A| \leq |A \times B| \leq |A|$ and hence $|A| = |A \times B|$. It follows that $\mathcal{P}(A)$ and $\mathcal{P}(A \times B)$ are equinumerous.

Note that $B^A \subseteq \mathcal{P}(A \times B)$. So we have $|B^A| \leq |\mathcal{P}(A)| = |2^A|$. As $2 \leq |B|$ we have an injective function $2^A \to B^A$. The required equalities now follow.

[3] Using Zorn's Lemma (or otherwise), prove the following.

(i) Suppose $(A; \leq_1)$ is any partially ordered set. Prove that there is a linearly ordered set $(A; \leq_2)$ with the property that for all $a, a' \in A$ we have $a \leq_1 a'$ implies $a \leq_2 a'$.

(ii) Let R be any (commutative) ring with identity element and $I \subset R$ be a proper ideal of R. Then there is a maximal proper ideal J of R with $I \subseteq J \subset R$.

(iii) Suppose G is a non-trivial group with an element g whose conjugates generate G. Prove that G has a maximal proper normal subgroup. Is this necessarily true without assuming the existence of such an element g?

Solution: (i) Consider the subset P of $\mathcal{P}(A^2)$ consisting of 2-ary relations R which are linear orderings of subsets of A with the property that for all $a, a' \in A$, if $R(a, a')$ holds, then $a \leq_1 a'$. Then $(P; \subseteq)$ is a non-empty partially ordered set and if $U \subseteq P$ is a chain in $(P; \subseteq)$ it is easy to see that $\bigcup U \in P$ is an upper bound for the elements of U. Thus by Zorn's Lemma there is a maximal element R of P. By assumption this is a linear ordering of a subset B of A and if $R(b, b')$ holds, then $b \leq_1 b'$. It will suffice to prove that $B = A$. For readability of notation, write $b \leq_R b'$ instead of $R(b, b')$.

Suppose $a \in A \setminus B$. We define a reflexive binary relation $S \supseteq R$ on $B \cup \{a\}$ as follows, again denoting it by $\leq_S$. For $b \in B$ we say that $b \leq_S a$ if there is $b' \in B$ with $b \leq_R b' \leq_1 a$. Otherwise we define $a \leq_S b$. We then check that $\leq_S$ is a linear ordering on $B \cup \{a\}$ which is in P. This contradicts the maximality of R, so we have $A = B$, as required. The main thing to check is that $\leq_S$ is transitive. This involves a bit of case splitting. For example, if $b_1, b_2 \in B$ and $b_1 \leq_S b_2 \leq_S a$ there is $b' \in B$ with $b_2 \leq_R b' \leq_1 a$ so $b_1 \leq_R b' \leq_1 a$ and therefore $b_1 \leq_S a$. You can complete the rest of the details yourself.

(ii) Note that an ideal of R is proper iff it does not contain the identity element 1 of R. Consider the poset P of proper ideals J with $I \subseteq J \subset R$, ordered by inclusion. This is non-empty (as $I \in P$) and if $C \subseteq P$ is a chain, then $J = \bigcup C$ is an ideal containing I and every element of C. Moreover it is proper as $1 \notin \bigcup C$. So $\bigcup C \in P$ is an upper bound for C. Hence by Zorn's Lemma, P has a maximal element. This is a maximal proper ideal containing I.

(iii) Note that if N is a normal subgroup of G which contains g, then $N = G$. Let P be the set of normal subgroups of G which do not contain g. This is a poset, ordered by inclusion. It is non-empty as it contains the identity subgroup. If C is a chain in P, then $\bigcup C$ is a normal subgroup of G; moreover, it is proper as $g \notin \bigcup C$. So $\bigcup C \in P$ is an upper bound for C in P. By Zorn's Lemma, P has a maximal element N. So $N \lhd G$ and if M is a normal subgroup of G properly containing N, then $M \notin P$, so $g \in M$. Therefore $M = G$. Thus N is a maximal proper normal subgroup of G.

Without the assumption that G has such an element g, it can happen that G has no maximal proper normal subgroup. For example, take G to be $(\mathbb{Q}; +)$, the additive group of the rational numbers. If H were a proper maximal (normal) subgroup then the quotient group G/H would be a non-trivial, simple abelian group. So it would be cyclic of prime order. But G/H has the property (divisibility) that every element has an n-th root in the group, for every natural number n (as the same is true in G) and this does not happen in a cyclic group of prime order. So there is no such subgroup H.

[4] In this question, assume ZF. We will show that Zorn's Lemma implies the Axiom of Choice: that is, $ZF \vdash (ZL \to AC)$.

Suppose X is a set of non-empty sets. By a *partial choice function* on X, with domain $Y \subseteq X$, we mean a function $f : Y \to \bigcup X$ with $f(y) \in y$ for all $y \in Y$. We let A be the set of all partial choice functions on X and we order these by inclusion $\subseteq$.

(i) Suppose $C \subseteq A$ is a chain in A. Prove that $\bigcup C \in A$.

(ii) Show that if the domain of $f \in A$ is not equal to X, then f is not maximal in A.

(iii) Deduce that if Zorn's Lemma holds, then there is a function $g : X \to \bigcup X$ with $g(x) \in x$ for all $x \in X$.

Solution:

(i) Let $F = \bigcup C$. Certainly F is a subset of $X \times \bigcup X$. To show that it is a function, suppose $(a, b_1), (a, b_2) \in F$. There exist $f_1, f_2 \in C$ with $(a, b_i) \in f_i$. As C is a chain in A, we may assume without loss of generality that $f_1 \subseteq f_2$. As f_2 is a partial choice function it follows that $b_1 = b_2$ and $b_2 = f_2(a) \in a$. So F is a partial choice function, as required.

(ii) Suppose $x \in X$ is not in the domain of f. Then for every $y \in x$, the set $g_y = f \cup \{(x, y)\}$ is in A and $f \subset g_y$. As $x \neq \emptyset$, we deduce that f is not maximal in A.

(iii) By (i), the poset $(A; \subseteq)$ satisfies the hypotheses of Zorn's Lemma, so has a maximal element g. By (ii), the domain of g is X, as required.

[5] Suppose κ is a cardinal with $\kappa > |\mathbb{R}|$. Prove that there is a vector space V over $\mathbb{R}$ with $|V| = \kappa$. (You could use the Löwenheim - Skolem Theorem here, but it's probably also instructive to try to do this directly.) Prove that a basis of V has cardinality κ.

Prove that if V_1, V_2 are $\mathbb{R}$-vector spaces with $|V_1| = |V_2| > |\mathbb{R}|$ then there is a bijective linear map $T : V_1 \to V_2$ (i.e. V_1, V_2 are isomorphic).

Solution: Suppose V is an $\mathbb{R}$-vector space with $|V| > |\mathbb{R}|$. Let B be a basis of V. Then by the argument in 4.3.4 of the notes, $|B| = |V|$. It follows from this that if $B_0 \subseteq B$ is such that $|B_0| > |\mathbb{R}|$, then the subspace W of V spanned by B_0 has cardinality $|B_0|$.

Thus, to prove that there is an $\mathbb{R}$-vector space of cardinality $\kappa > |\mathbb{R}|$ it is enough to show that there is an $\mathbb{R}$-vector space of cardinality $\geq \kappa$ (we can then take a subspace, with a basis of cardinality κ). There are various ways to do this. Note that for any set X, the set $\mathbb{R}^X$ of functions $X \to \mathbb{R}$ is an $\mathbb{R}$-vector space (under addition of functions). By 4.2.9 in the notes, if $\lambda = |X| \geq |\mathbb{R}|$, then this has cardinality 2^λ. So take X to be any set of cardinality κ here.

For the final part, if V_1, V_2 are $\mathbb{R}$-vector spaces with $|V_1| = |V_2| > |\mathbb{R}|$ and B_1, B_2 are bases of V_1, V_2 respectively, then $|B_1| = |B_2|$, so there is a bijection $h : B_1 \to B_2$. As B_1 is a basis of V_1, there is a unique linear map $T : V_1 \to V_2$ with $T(v) = h(v)$ for all $v \in B_1$. As B_2 is a basis of V_2, T is bijective.

[5] Let A be a non-empty set. A set F of subsets of A is called a *filter* on A if it satisfies the first three of the following properties. If it satisfies all four, it is called an *ultrafilter* on A.

UF1 $\emptyset \notin F$;

UF2 if $x \in F$ and $x \subseteq y \subseteq A$, then $y \in F$;

UF3 if $x, y \in F$ then $x \cap y \in F$;

UF4 if x is any subset of A then either x or its complement $A \setminus x$ is in F.

(i) (Nothing to do with Zorn's Lemma) Suppose A is a finite set and F an ultrafilter on A. Show that there exists $a \in A$ such that $F = \{x \subseteq A : a \in x\}$.

(ii) Show that if A is an infinite set the the set of subsets whose complements are finite forms a filter on A.

(iii) Show that if F_0 is a filter on A then the set of filters which contain it is a poset (under inclusion) which satisfies the hypotheses of Zorn's Lemma.

(iv) Show that a maximal filter satisfies (UF4).

(v) Let F be a maximal filter containing the filter in (ii). Show that F does not contain any finite set.

Solution: (i) Let $x \in F$ have minimal cardinality. By (UF1), $x \neq \emptyset$, so let $a \in x$. By (UF4), either $\{a\}$ or $A \setminus \{a\}$ is in F. In the second case, $(A \setminus \{a\}) \cap x \in F$ (by UF3), contradicting the choice of x. So $x = \{a\}$ and it follows that $F = \{y \subseteq A : a \in y\}$, as required.

(ii) By De Morgan's Law.

(iii) This is straightforward, similar to the examples in question 2.

(iv) Suppose F is a maximal filter on A and $x \subseteq A$ is such that $x \notin F$. We show $A \setminus x \in F$. Consider

$$E = \{z \subseteq A : z \supseteq x \cap y \text{ for some } y \in F\}.$$

This properly contains F and satisfies UF2 and UF3. So by maximality of F, we have $\emptyset \in E$. Thus there is $y \in F$ with $\emptyset = x \cap y$, so $A \setminus x \supseteq y$ and therefore $A \setminus x \in F$.

(v) This follows from UF1, UF3 and the fact that F contains the complements of all finite subsets of A.