.1 Intermezzo: Zorn's lemma

Problem .1.1. Prove that every well-ordering is total.

Solution. Recall that a well-ordering on Z is an order relation such that every nonempty subset of Z has a least element. For any two elements $a, b \in Z$, consider the subset $\{a, b\} \subseteq Z$. Since this subset has a least element, it must be the case that either $a \preceq b$ or $b \preceq a$. As this holds for any pair of elements in Z, it follows that $\preceq$ is total on Z. □

Problem .1.2. Prove that a totally ordered set $(Z, \preceq)$ is a woset if and only if every descending chain

$$z_1 \succeq z_2 \succeq z_3 \succeq \cdots$$

in Z stabilizes.

Solution. Suppose every such descending chain stabilizes. Let $S \subseteq Z$ be a nonempty subset. Since Z is totally ordered, the elements of S form a descending chain as described above. Then there is some element a such that for all $b \in Z$, $a \preceq b$. That is, a is a least element in S. Then Z is well-ordered.

Now suppose Z is a woset. Assume there is a descending chain which does not stabilize. Then the set formed by these elements does not have a minimum element, a contradiction. Therefore, every descending chain in Z stabilizes. □

Problem .1.3. Prove that the axiom of choice is equivalent to the statement that a set-function is surjective if and only if it has a right-inverse (cf. Exercise I.2.2).

Solution. The proof of the statement about surjective set-functions assumes the axiom of choice, showing that it is sufficient. To see that it is necessary, assume that every surjective set-function has a right-inverse. Let A be a set of disjoint nonempty sets and $B = \bigcup A$. Then for each $b \in B$, there exists exactly one set $X \in A$ such that $b \in X$. Thus, we have a surjective function $f : B \to A$. Then it has a right-inverse g. Define $C := \{g(X) \mid X \in A\}$. Then C is a choice set. □

Problem .1.4. Construct explicitly a well-ordering on $\mathbb{Z}$. Explain why you know that $\mathbb{Q}$ can be well-ordered, even without performing an explicit construction.

Solution. The well-ordering on $\mathbb{N}$, namely $\leq$, does not work because of the negative numbers so we work around this by imposing conditions. Let $a, b \in \mathbb{Z}$ and set $a \preceq b$ if and only if one of the following holds:

- $|a| < |b|$.
- $|a| = |b|$ and $a \leq b$.

This well ordering yields the following visualization: $0, -1, 1, -2, 2, \ldots$ Assuming the Well-ordering Theorem, every set admits a well-ordering, including $\mathbb{Q}$. Without directly invoking the theorem, we also know that $\mathbb{Q}$ is a countable set and thus is in bijection with $\mathbb{N}$, which has a well-ordering. □

Problem .1.5. Prove that the (ordinary) principle of induction is equivalent to the statement that $\leq$ is a well-ordering on $\mathbb{Z}^{>0}$. (To prove by induction that $(\mathbb{Z}^{>0}, \leq)$ is well-ordered, assume it is known that 1 is the least element of $\mathbb{Z}^{>0}$ and that $\forall n \in \mathbb{Z}^{>0}$ there are no integers between n and $n+1$.)

Solution. In Claim 3.2, it was shown that the principle of induction holds for any well-ordered set. That is, $\leq$ being a well-ordering on $\mathbb{Z}^{>0}$ implies that the principle of induction holds. To show the converse, we can assume that 1 is the least element of $\mathbb{Z}^{>0}$ and that there are no integers between n and $n+1$ for all $n \in \mathbb{Z}$. Suppose that there exist a non-empty subset S of $\mathbb{Z}^{>0}$ such that S has no minimum element. Then $1 \notin S$ or else it would be a minimal element. Similarly, $2 \notin S$ because there are no integers between 1 and 2, which would make 1 a minimal element. If none of $1, 2, \ldots, n$ are in S, then $n+1 \notin S$ or it would be minimal. Thus, the principle of induction implies that S is empty, a contradiction. Therefore, S must have a minimal element so $\leq$ is a well-ordering on $\mathbb{Z}^{>0}$. □

Problem .1.6. In this exercise assume the truth of Zorn's lemma and the conventional set-theoretic constructions; you will be proving the well-ordering theorem.

Let Z be a nonempty set, and let $\mathscr{Z}$ be the set of pairs $(S, \leq)$ consisting of a subset S of Z and of a *well-ordering* $\leq$ on S. Note that $\mathscr{Z}$ is not empty (singletons can be well-ordered). Define a relation $\preceq$ on $\mathscr{Z}$ by prescribing

$$(S, \leq) \preceq (T, \leq')$$

if and only if $S \subseteq T, \leq$ is the restriction of $\leq'$ to S, and every element of S precedes every element of $T \setminus S$ w.r.t. $\leq'$.

- Prove that $\preceq$ is an order relation in $\mathscr{Z}$.
- Prove that every chain in $\mathscr{Z}$ has an upper bound in $\mathscr{Z}$.
- Use Zorn's lemma to obtain a maximal element $(M, \leq)$ in $\mathscr{Z}$. Prove that $M = Z$.

Thus every set admits a well-ordering, as stated in Theorem 3.3.

Solution. Recall that an order relation is reflexive, transitive, and antisymmetric. Given a pair $(S, \leq)$, certainly we have $S \subseteq S$ and every element of S precedes every element of $S \setminus S = \emptyset$ with respect to $\leq$. Therefore, $\preceq$ is reflexive. Let $(T, \leq'), (R, \leq'') \in \mathscr{Z}$ such that $(S, \leq) \preceq (T, \leq')$ and $(T, \leq') \preceq (R, \leq'')$. Then $S \subseteq R$ (by transitivity of subsets) and $\leq$ is the restriction of $\leq'$ to S, which is the restriction of $\leq''$ to S. Furthermore, $S \subseteq T$ and every element of T precedes every element of $R \setminus T$ w.r.t. $\leq''$. In particular, every element of S precedes the elements of $R \setminus T$ w.r.t. $\leq''$. Thus, we have $(S, \leq) \preceq (R, \leq'')$, proving transitivity. Finally, suppose we have $(S, \leq) \preceq (T, \leq')$ and $(T, \leq') \preceq (S, \leq)$. Then $S \subseteq T$ and $T \subseteq S$ so $S = T$. To show the two order relations are equivalent, let $a, b \in S$ such that $a \leq b$. Since $\leq$ is the restriction of $\leq'$, we have $a \leq' b$. Similarly, we find $a \leq' b \Longrightarrow a \leq b$. Thus, the two order relations are equivalent and we find $(S, \leq) = (T, \leq')$, proving antisymmetry and showing that $\preceq$ is in fact an order relation on $\mathscr{Z}$.

Now consider a chain $\mathscr{C}$ of subsets. We must show it has an upper bound in $\mathscr{Z}$. Consider the set

$$U := \bigcup_{S \in \mathscr{C}} S.$$

Certainly each $S \subseteq U$. Furthermore, there is a natural order relation on U since for all $a, b \in U$, there exists some $S \in \mathscr{C}$ containing both a and b. Then the order relation on S has $a \leq b$ which also holds in U. Thus, U is well-ordered and is an upper bound for $\mathscr{C}$.

Since every chain has an upper bound, Zorn's lemma states that there is a maximal element $(M, \leq)$ in $\mathscr{Z}$. Clearly $M \subseteq Z$. To show that $M = Z$, suppose otherwise. That is, suppose there is some element $x_0 \in Z \setminus M$. Then consider the set $M \cup \{x_0\}$ with the order relation $\leq'$ such that for all $x \in M$, $x \leq' x_0$. Then $(M, \leq) \preceq (M \cup \{x_0\}, \leq')$, contradicting the maximality of M. Thus, $M = Z$ so Z has a well-ordering. □

Problem .1.7. In this exercise assume the truth of the axiom of choice and the conventional set-theoretic constructions; you will be proving the well-ordering theorem.

Let Z be a nonempty set. Use the axiom of choice to choose an element $\gamma(S) \notin S$ for each proper subset $S \subsetneq Z$. Call a pair $(S, \leq)$ a γ-*woset* if $S \subseteq Z$, $\leq$ is a well-ordering on S, and for every $a \in S$, $a = \gamma(\{b \in S, b < a\})$.

- Show how to begin constructing a γ-woset, and show that all γ-wosets must begin in the same way.

Define an ordering on γ-wosets by prescribing that $(U, \leq'') \preceq (T, \leq')$ if and only if $U \subseteq T$ and $\leq''$ is the restriction of $\leq'$.

- Prove that if $(U, \leq'') \prec (T, \leq')$, then $\gamma(U) \in T$.
- For two γ-wosets $(S, \leq)$ and $(T, \leq')$, prove that there is a maximal γ-woset $(U, \leq'')$ preceding both w.r.t. $\preceq$. (Note: There is no need to use Zorn's lemma!)

- Prove that the maximal γ-woset found in the previous point in fact equals $(S, \leq)$ or $(T, \leq')$. Thus, $\preceq$ is a total ordering.
- Prove that there is a maximal γ-woset $(M, \leq)$ w.r.t. $\preceq$. (Again, Zorn's lemma need not and should not be invoked.)
- Prove that $M = Z$.

Thus every set admits a well-ordering, as stated in Theorem 3.3.

Solution. Given $\gamma(S)$, one can begin constructing a γ-woset $(S, \leq)$ by including $\gamma(\emptyset)$. In some sense, $a = \gamma(\emptyset)$ is minimal in S since no elements precede it. Furthermore, since every γ-woset is well-ordered, they all have a minimal element. That is, they all contain $\gamma(\emptyset)$. One can continue the construction of the γ-woset by letting the next element be γ of the elements currently in the set. The well-ordering on the set follows naturally.

Now suppose we have $(U, \leq'') \prec (T, \leq')$. By the definition of $\prec$, we have $U \subset T$. Since T is well-ordered, there is some minimum element a such that for all $b \in U$, $b <' a$. Then $a = \gamma(\{b \in S, b <' a\}) = \gamma(U)$.

Given two γ-wosets $(S, \leq)$ and $(T, \leq')$, consider the set $R = S \cap T$ with the obvious well ordering. Indeed, since $R \subseteq S$ and $R \subseteq T$, R precedes both w.r.t. $\preceq$. Furthermore, if there were any more elements then it would not satisfy the defining property of being a subset of both S and T so it is maximal.

If $R = S$, then there is nothing to prove so suppose otherwise. Then $R \prec S$ so $\gamma(R) = a \in S$ for some s. If $R \prec T$ then $\gamma(R) = b \in T$ for some b. But then $a = b \in S \cap T = R$, a contradiction (since $\gamma(R) \notin R$). Thus, $R = S$ or $R = T$ and $\preceq$ is a total ordering.

Since $\preceq$ is a total ordering, we can construct a chain of γ-wosets. Let M be the union of these γ-wosets with the ordering inherited from the wosets. Certainly each γ-woset $S \subseteq M$ so M is maximal.

Finally, we know $M \subseteq Z$. Suppose $Z \subsetneq M$. Then there exists some element $x \in Z \setminus M$. Consider $M \cup \{x\}$. Since $\gamma(\{x\})$ is defined, this set is a γ-woset properly containing M, contradicting the maximality of M. Thus, $M = Z$ so there is a well-ordering on Z. $\square$

Problem .1.8. Prove that every nontrivial finitely generated group has a maximal proper subgroup. Prove that $(\mathbb{Q}, +)$ has no maximal proper subgroup.

Solution. Let $\mathscr{S}$ be the set of all proper subgroups of a finitely generated group G. Then $\mathscr{S}$ is partially ordered by inclusion so let $\mathscr{C}$ be a chain in this poset. Let H be the union of all subgroups in this chain. Since the chain is nonempty, there is one subgroup K_0 containing the identity, so H contains the identity. Furthermore, suppose $x, y \in H$. Then there are subgroups K_1, K_2 with $x \in K_1$, $y \in K_2$. Suppose WLOG that $K_1 \subseteq K_2$. Then both $x, y \in K_2$ and since K_2 is a subgroup, $xy^{-1} \in K_2 \subseteq H$. Thus H is a subgroup.

To show H is a proper subgroup, suppose otherwise. In particular, H contains the generators $g_1, g_2, \dots, g_n$ of G. Then there is some subgroup K_n containing all such generators, implying that $K_n = G$, a contradiction. Thus, H must be proper.

Since every chain in $\mathscr{S}$ has an upper bound in $\mathscr{S}$, Zorn's lemma applies and $\mathscr{S}$ has a maximal element. That is, G has a maximal proper subgroup.

Suppose that $(\mathbb{Q}, +)$ has a maximal proper subgroup H. Then the quotient $\mathbb{Q}/H$ is simple and abelian, so it must be cyclic with prime order. Say $\mathbb{Q}/H \cong \mathbb{Z}/p\mathbb{Z}$. Choose $x \in \mathbb{Q} \setminus H$. Then $H = p(\frac{x}{p} + H) = x + N$, implying that $x \in N$, a contradiction. Thus, $\mathbb{Q}$ has no maximal proper subgroup. □

Problem .1.9. Consider the rng (= ring without 1; cf. §III.1.1) consisting of the abelian group $(\mathbb{Q}, +)$ endowed with the trivial multiplication $qr = 0$ for all $q, r \in \mathbb{Q}$. Prove that this rng has no maximal ideals.

Solution. Suppose the ring R has a maximal ideal M. Then M is also a maximal subgroup of $\mathbb{Q}$ (a larger subgroup would also act as an ideal). As shown above, $\mathbb{Q}$ does not contain maximal subgroups so neither can M be a maximal ideal. □

Problem .1.10. As shown in Exercise III.4.17, every maximal ideal in the ring of continuous real-valued functions on a *compact* topological space K consists of the functions vanishing of a point of K.

Prove that there are maximal ideals in the ring of continuous real-value functions on the *real line* that do not correspond to points of the real line in the same fashion. (Hint: Produce a proper ideal that is not contained in any maximal ideal corresponding to a point, and apply Proposition 3.5.)

Solution. I still don't know topology but I imagine the solution uses something about the fact that the real line is not compact (whatever that means). □

Problem .1.11. Prove that a UFD R is a PID if and only if every nonzero prime ideal in R is maximal. (Hint: One direction is Proposition III.4.13. For the other, assume that every nonzero prime ideal in a UFD R is maximal, and prove that every maximal ideal in R is principal; then use Proposition 3.5 to relate arbitrary ideals to maximal ideals, and prove that every ideal of R is principal.)

Solution. First suppose that R is a PID and let $I = (a)$ be a nonzero prime ideal. Assume $I \subseteq J$ for an ideal $J = (b)$ of R. Since $a \in (b)$, we have $a = bc$ for some $c \in R$. But since a is prime, we have $b \in (a)$ or $c \in (a)$. In the first case, there is nothing more to prove. In the second, we have $c = da$. Then

$$a = bda \Longrightarrow bd = 1 \Longrightarrow (b) = (1) = R.$$

Thus, I is maximal.

Now let R be a UFD such that every prime ideal is maximal. Let I be a maximal ideal. Then I is also a prime ideal of height 1. By Exercise 2.9, I is principal. Thus, every maximal ideal is principal. Now let I_0 be an arbitrary ideal. It is contained in some maximal ideal $\mathfrak{m}_0 = (a_0)$. In particular, every element admits a factor of a, which is irreducible (by Exercise 1.12). Then we may write $I = a_0 J_0$ for an ideal J_0. If $J_0 = R$ then $I = (a_0)$ and we are done. Otherwise, J_0 is properly contained in a maximal ideal $\mathfrak{m}_1 = (a_1)$ so we may write $J_0 = a_1 J_1$. We may repeat this and it will terminate since the elements of I only have finitely many irreducible factors. When it terminates, we find that $J_t = R$ so $I = (a_0 a_1 \cdots a_t)$. □

Problem .1.12. Let R be a commutative ring, and let $I \subseteq R$ be a proper ideal. Prove that the set of prime ideals containing I has minimal elements. (These are the *minimal primes* of I.)

Solution. Consider the set $\mathscr{I}$ of prime ideals of R which contain I. The set is ordered by inclusion so consider a chain $\mathscr{C}$ and let $\mathfrak{B}$ be the intersection of the prime ideals in $\mathscr{C}$. Certainly $I \subseteq \mathfrak{B}$. Now we must check that $\mathfrak{B}$ is in fact prime. Suppose $ab \in \mathfrak{B}$ but neither a nor b is. Then there exist two prime ideals $\mathfrak{p}, \mathfrak{p}'$ such that $a \notin \mathfrak{p}, b \notin \mathfrak{p}'$ and WLOG $\mathfrak{p} \subseteq \mathfrak{p}'$. Then $a, b \notin \mathfrak{p}$ but $ab \in \mathfrak{p}$, contradicting that $\mathfrak{p}$ is prime. Thus, $\mathfrak{B}$ is prime. Since every chain in $\mathscr{I}$ has a lower bound, $\mathscr{I}$ has a minimal element. □

Problem .1.13. Let R be a commutative ring, and let N be its nilradical (Exercise III.3.12). Let $r \notin N$.

- Consider the family $\mathscr{F}$ of ideals of R that do not contain any power r^k of r for $k > 0$. Prove that $\mathscr{F}$ has maximal elements.
- Let I be a maximal element of $\mathscr{F}$. Prove that I is prime.
- Conclude $r \notin N \Longrightarrow r$ is not in the intersection of all prime ideals of R.

Together with Exercise III.4.18, this shows that the nilradical of a commutative ring R equals the intersection of all prime ideals of R.

Solution. Recall that the nilradical of a ring is the set of nilpotent elements (elements a such that $a^n = 0$ for some n). The nilradical is an ideal of R.

The family $\mathscr{F}$ of ideals not containing any power of r^k is ordered by inclusion. Each chain in this family has a maximal element, namely the union of all of the ideals in the chain. Therefore, by Zorn's lemma $\mathscr{F}$ has maximal elements.

Let I be a maximal element of $\mathscr{F}$ and suppose $ab \in I$ but $a, b \notin I$. Then the ideals $I + (a)$ and $I + (b)$ both properly contain I. By the maximality of I, we have $r^m \in I + (a)$ and $r^n \in I + (b)$. But then we find

$$r^{m+n} = (s_1 + ax)(s_2 + by) = s_1 s_2 + s_1 \cdot by + ax \cdot s_2 + ax \cdot by \in I$$

for $s_1, s_2 \in I$, a contradiction. Thus one of $a, b \in I$ so I is prime.

Suppose r is not in the nilradical of R. Then there is some prime ideal not containing any power of r, so r is not in the intersection of all prime ideals. In particular, $\bigcap \mathfrak{p} \subseteq N$. $\square$

Problem .1.14. The *Jacobson radical* of a commutative ring R is the intersection of the maximal ideals in R. (Thus, the Jacobson radical contains the nilradical.) Prove that r is in the Jacobson radical if and only if $1 + rs$ is invertible for every $s \in R$.

Solution. If r is in the Jacobson radical, then it is in every maximal ideal. Suppose there exists some $s \in R$ such that $1 + rs$ is not invertible. Then $(1 + rs)$ is a proper ideal and hence is contained in a maximal ideal $\mathfrak{m}$. But $r \in \mathfrak{m}$ so $1 = rs - r \cdot s \in \mathfrak{m}$, a contradiction. Thus $1 + rs$ is invertible for all $s \in R$.

Now suppose that $1 + rs$ is invertible for all $s \in R$ and let $\mathfrak{m}$ be a maximal ideal. If $r \notin \mathfrak{m}$ then $\mathfrak{m} + (r) = R$ so there exists $y \in \mathfrak{m}$ and $s \in (r)$ such that $rs + y = 1$. But then $y = 1 - rs$ is invertible so $1 = yy^{-1} \in \mathfrak{m}$, a contradiction. Thus, $r \in \mathfrak{m}$. $\square$

Problem .1.15. Recall that a (commutative) ring R is Noetherian if every ideal of R is finitely generated. Assume the seemingly weaker condition that every *prime* ideal of R is finitely generated. Let $\mathscr{F}$ be the family of ideals that are not finitely generated in R. You will prove $\mathscr{F} = \emptyset$.

- If $\mathscr{F} \neq 0$, prove that it has a maximal element I.
- Prove that R/I is Noetherian.
- Prove that there are ideals J_1, J_2 properly containing I, such that $J_1 J_2 \subseteq I$.
- Give a structure of R/I module to I/J_1J_2 and J_1/J_1J_2.
- Prove that I/J_1J_2 is a finitely generated R/I-module.
- Prove that I is finitely generated, thereby reaching a contradiction.

Thus, a ring is Noetherian if and only if its *prime* ideals are finitely generated.

Solution. If $\mathscr{F}$ is nonempty, it is partially ordered by inclusion. For each chain $\mathscr{C}$ in $\mathscr{F}$, the ideal defined as the union of ideals in the chain is an upper bound for $\mathscr{C}$. Indeed, if it were finitely generated then the generating set would be contained in one of the ideals, contradicting the assumption that ideals in $\mathscr{F}$ are not finitely generated. By Zorn's lemma, $\mathscr{F}$ has maximal elements. Let I be one such maximal element.

Suppose R/I is not Noetherian. That is, there is some ideal of the form J/I which is not finitely generated. Then J is an ideal of R containing I and it is not finitely generated. But by the maximality of I, we have $J = R$ which is finitely generated by 1, a contradiction. Thus R/I is Noetherian.

Since I is not finitely generated, it is not prime. Thus, there exist elements $a, b \notin I$ with $ab \in I$. Then $J_1 = I + (a)$ and $J_2 = I + (b)$ both properly contain I (and thus are finitely generated) and elements of $J_1 J_2$ are of the form

$$(r_1 + ax)(r_2 + by) = r_1 \cdot r_2 + r_1 \cdot by + r_2 \cdot ax + ab \cdot xy \in I,$$

so $J_1 J_2 \subseteq I$.

We can give the quotient $I/J_1 J_2$ the structure of an R/I module by defining

$$(r + I)x = rx$$

for $r \in R$ and $x \in I/J_1 J_2$. Indeed, since $x = a + J_1 J_2$ for $a \in I$, we find

$$r(a + J_1 J_2) = ra + rJ_1 J_2 \in \frac{I}{J_1 J_2}$$

The other module axioms can be checked easily. We can define the same structure on $J_1/J_1 J_2$.

Recall that J_1 is finitely generated. Then $J_1/J_1 J_2$ is also finitely generated over R and hence over R/I. Since R/I is Noetherian and $I/J_1 J_2$ is a submodule of $J_1/J_1 J_2$, we find that $I/J_1 J_2$ is finitely generated.

Finally, observe that $J_1 J_2 \subseteq I$ is finitely generated and $I/J_1 J_2$ is finitely generated. Thus, I is finitely generated and we arrive at a contradiction. Therefore, a ring is Noetherian if and only if its prime ideals are finitely generated. $\square$