Chapter 4. Cardinal Arithmetic.*

4.1. Basic notions about cardinals.

We are used to comparing the size of sets by seeing if there is an injection from one to the other, or a bijection between the two.

Definition. Let x, y be sets. Le $x \preceq y$ if there is an injection of x into y (*i.e.* a function f such that for all z_0, $z_1 \in x$ we have que $f(z_0) = f(z_1) \Longrightarrow z_0 = a_1$).
and let $x \preceq^* y$ either if $x = \emptyset$ or if there is a surjection from y to x (*i.e.* a function g such that for all $z \in x$ there is $u \in y$ such that $g(u) = z$).
Define $x \sim y$ if there is a bijection $f : x \longrightarrow y$ (*i.e.* a function f from x to y such that f is an injection and a surjection.

Our first two Lemmas are straightforward.

Lemma. If $x \preceq y$, then $x \preceq^* y$

Proof. If $x = \emptyset$ there is nothing to show. Otherwise let $f : x \longrightarrow y$ be an injection and let u be any arbitrary element of x. Then, if we define $g : y \longrightarrow x$ by $g(z) = f^{-1}(z)$ if $z \in \mathrm{im}(f)$, and $g(z) = u$ is otherwise, it is clear that g is a surjection.

Lemma. AC implies that if $x \preceq^* y$, then $x \preceq y$.

Proof. If $g : y \longrightarrow x$ is a surjection, let $s_v = \{u \in y \,|\, g(u) = v\}$ for all $v \in x$ and let $z = \{s_v \,|\, v \in x\}$. We apply AC to z. This gives us a function $f : z \longrightarrow \bigcup z, = y$, such that $f(s_v) \in s_v$ for all $s_v \in z$. So the function $h : x \longrightarrow y$ defined by $h(v) = f(s_v)$ is an injection, because if we have v_0, $v_1 \in x$ and $h(v_0) = h(v_1)$, then $v_0 = g(h(v_0)) = g(h(v_1)) = v_1$.

Note. We need AC to establish this fact. However the following theorem does *not* use the axiom of choice.

Theorem. (Schröder-Bernstein) If $x \preceq y$ and $y \preceq x$, then $x \sim y$.

Proof. Suppose that $i : x \longrightarrow y$ and $j : y \longrightarrow x$ are injections. Define $k : \mathcal{P}(x) \longrightarrow \mathcal{P}(x)$ by $k(a) = (x \setminus j``y) \cup j{\cdot}i``a$ for each $a \in x$. It is clear that if $a \subseteq b \subseteq x$, then $k(a) \subseteq k(b)$.

Take $c = \bigcup\{a \subseteq x \,|\, a \subseteq k(a)\}$. Then $c \subseteq \bigcup\{k(a) \,|\, a \subseteq x \;\&\; a \subseteq k(a)\} \subseteq k(c)$, because $a \subseteq k(a) \subseteq k(c)$ when $a \subseteq c$. So $k(c) \subseteq k(k(c))$. Thus $k(c) \subseteq c$, and $c = k(c)$. (Note that up to here we have only used that k is increasing on $\mathcal{P}(x)$ and nothing more.)

Define $f : x \longrightarrow y$ by $f(u) = i(u)$ if $u \in c$, and $f(u) = j^{-1}(u)$ if $u \notin c$. Let u_0, $u_1 \in x$. If both u_0, $u_1 \in c$ it is clear that $f(u_0) = f(u_1)$ implies $u_0 = u_1$. Similarly, if u_0, $u_1 \notin c$ we have that $f(u_0) = f(u_1)$ implies $u_0 = u_1$ as well. And if $u_0 \in c$ and $u_1 \notin c$ and $f(u_1) = v$, then $v \notin \mathrm{im}(i)$ and $f(u_0) \neq f(u_1)$. Finally, if $v \in y$ and there is no $u \in c$ such that $f(u) = v$, then $j(v) \notin c$ and $v = f(j(v))$.

Definition. A *notion of cardinality* is a function, $\mathrm{card} : V \longrightarrow V$, such that $\mathrm{card}(x) = \mathrm{card}(y)$ if and only if $x \sim y$.

* version 1.0, 24/1/06

Even without AC there are such notions. We will use one, for which we will write $\overline{\overline{x}}$ instead of card(x):

$$\overline{\overline{x}} = \alpha \text{ where } \alpha \in \mathrm{On} \text{ is minimal such that there is a well-order of } x \text{ bijective with } \alpha, \text{ if there is such an } \alpha, \text{ and}$$

$$\overline{\overline{x}} = V_\alpha \cap \{y \mid y \sim x\} \text{ where } \alpha \text{ is minimal such that there is } y \in V_\alpha \text{ with } y \sim x, \text{ otherwise.}$$

Note. We make this definition in the case that there is no well-order of x because it would not be desirable to use the equivalence class of x under $\sim$, since this is a proper class.

With the axiom of choice the equivalent well-ordering principle (WO) says that any set can be well-ordered, and so by §2.6 for any set there is an ordinal with which it is in bijection. Hence under AC the cardinality of any set is an ordinal.

Exercise. Show that $\overline{\overline{x}} \notin \mathrm{On}$ if there is no well-ordering of x.

Definition. (For any notion of cardinality.) A set $\mathbf{m}$ is a cardinal if there is some $x \in V$ such that card(x) $= \mathbf{m}$.

$\mathbf{m} \leq \mathbf{n}$ if there are x and y such that card(x) $= \mathbf{m}$ and card(y) $= \mathbf{n}$ and $x \preceq y$.

$\mathbf{m} + \mathbf{n} = \mathrm{card}(x \times \{0\} \cup y \times \{1\})$, where card($x$) $= \mathbf{m}$ and card(y) $= \mathbf{n}$.

$\mathbf{m} \,.\, \mathbf{n} = \mathrm{card}(x \times y)$, where card($x$) $= \mathbf{m}$ and card(y) $= \mathbf{n}$.

$\mathbf{m}^{\mathbf{n}} = \mathrm{card}({}^{y}x)$, where card($x$) $= \mathbf{m}$ and card(y) $= \mathbf{n}$.

Proposition. $+$ is commutative and associative; . is commutative, associative and distributive over $+$; and $\mathbf{m}^{\mathbf{n}+\mathbf{k}} = \mathbf{m}^{\mathbf{n}} \,.\, \mathbf{m}^{\mathbf{k}}$ and $(\mathbf{m}^{\mathbf{n}})^{\mathbf{k}} = \mathbf{m}^{\mathbf{n}\cdot\mathbf{k}}$.

Proof. All are immediate from the definitions.

Some other consequences are provable without the axiom of choice, but mainly involve $\preceq$ and/or $\preceq^*$.

Example. If $\mathbf{k} + \mathbf{r} = \mathbf{m} \,.\, \mathbf{n}$, then either $\mathbf{m} \preceq \mathbf{k}$ or $\mathbf{n} \preceq^* \mathbf{r}$.

4.2. Hartog's Lemma.

As we have seen, as with the axiom of choice we measure cardinality with ordinals, it is worthwhile establishing some relationships between ordinals and cardinals.

Hartog's Lemma. Let x be a set. Then $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\}$ is a set, and, so, is an element of On. ($\{\alpha \in \mathrm{On} \mid \alpha \sim x\}$ is also a set.) Moreover, $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\} \not\preceq x$ is the minimal ordinal with this property.

Proof. Let $W = \{(y, <) \mid y \subseteq x \;\&\; < \text{ is a well-order of } y\}$. Then W is a set (because it is a subset do $\mathcal{P}(x) \times \mathcal{P}(x \times x)$). As we saw in §2.6, by the strong recursion theorem and Replacement, there is a function, F, taking well-orders to ordinals. Thus, by Replacement, $F``W = \{\alpha \in \mathrm{On} \mid \alpha \preceq x\}$ is a set.

It is clear that $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\}$ is an initial segment of On, because if $\beta < \alpha \preceq x$ then a composition of the identity function with an injection from α to x is an injection from β to x. So $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\}$ is an element of On. Let $\{\alpha \in \mathrm{On} \mid \alpha \preceq x\} = \beta$. If $\beta \preceq x$ we have $\beta \in \beta$, a contradition! And it is clear that if $\gamma < \beta$ we have $\gamma \preceq x$.

From now on we always use this notation, $\overline{\overline{x}}$, for cardinality.

Proposition. (i) Let $\kappa \in \mathrm{On}$ be a cardinal. $\overline{\overline{\kappa}} = \kappa$. (ii) Let $\kappa \in \mathrm{On}$ be a cardinal. $\forall \alpha < \kappa\ \kappa \not\preceq \alpha$. (iii) Let α, $\beta \in \mathrm{On}$. Then $\overline{\overline{\alpha}} \leq \beta \leq \alpha$ implies that $\overline{\overline{\beta}} = \overline{\overline{\alpha}}$.

Proof. (i) Recall that to say that κ is a cardinal means that there is some x with a well-order and that κ is minimal such that $x \sim \kappa$. Choose such an x. $\kappa \sim \kappa$ and if $\alpha < \kappa$ and $\alpha \sim \kappa$ then $\alpha \sim x$, a contradition to the minimality of κ, because $\sim$ is an equivalence relation. So because κ itself is well-ordered (by $\in$) we have $\overline{\overline{\kappa}} = \kappa$.
(ii) If $\alpha < \kappa$ and $i : \kappa \longrightarrow \alpha$ is an injection, then $\mathrm{im}(i) \subseteq \alpha$ is isormorphic via an order-preserving isomorphism to a unique ordinal, let's say β, $\leq \alpha$. Thus $\beta < \kappa$ and $\beta \sim \kappa$.
(iii) $\beta \leq \alpha$ implies $\beta \subseteq \alpha$, so $\beta \preceq \alpha$. But $\alpha \sim \overline{\overline{\alpha}} \preceq \beta$, thus $\alpha \sim \beta$ by the Schröder-Bernstein Theorem.

Note. If $\kappa \in \omega \cup \{\omega\}$ we have that $\forall \alpha < \kappa\ \kappa \not\sim \alpha$, and so κ is a cardinal.

Definition. Let $\kappa \in \mathrm{On}$ be a cardinal. Define $\kappa^+ = \{\alpha \in \mathrm{On} \mid \alpha \preceq \kappa\}$.

Corollary to Hartog's Lemma. Then $\kappa^+ \in \mathrm{On}$, κ^+ is a cardinal, $\kappa < \kappa^+$, and $\kappa^+ \not\preceq \kappa$. And there is no $\beta \in \mathrm{On}$ such that $\beta < \kappa^+$ and β has these properties.

Proof. It is clear that $\kappa \in \kappa^+$. Apply Hartog's Lemma to $x = \kappa$ to see that κ^+ is an ordinal and $\kappa^+ \not\preceq \kappa$. If $\beta < \kappa^+$ we have that $\beta \preceq \kappa$, and so $\kappa^+ \not\sim \beta$. Thus $\overline{\overline{\beta}} \leq \kappa$ and κ^+ is a cardinal.

Corollary. There is no ordinal with maximal cardinality because $\overline{\overline{\alpha}} \leq \alpha < \overline{\overline{\alpha}}^+$ for any $\alpha \in \mathrm{On}$.

Definition. Let $\kappa \in \mathrm{On}$ be a cardinal. Then κ^+ is the cardinal successor of κ. We say that κ is a successor cardinal if there is a cardinal μ such that $\kappa = \mu^+$, and that κ is *a limit* cardinal otherwise.

Now we are going to enumerate those ordinals which are cardinals. The first ω are 0, 1, 2, ..., the natural numbers. After this we use the ordinals themselves to enumerate the infinite ordinals that are cardinals.

Definition. By recursion define $\aleph : \mathrm{On} \longrightarrow V$ (On) by $\aleph_\alpha = \omega \cup \{\gamma \in \mathrm{On} \mid \exists \beta < \alpha\, \gamma \preceq \aleph_\beta\}$. Also let us write ω_α instead of $\aleph_\alpha$ for any $\alpha \in \mathrm{On}$. ($\aleph$ is "aleph," the first letter of the hebrew alphabet.)

Proposition. (i) $\aleph_0 = \omega$. (ii) $\aleph_\alpha \in \mathrm{On}$ is a cardinal for each $\alpha \in \mathrm{On}$ (iii) if $\kappa \in \mathrm{On}$ is an infinite cardinal then there is an $\alpha \in \mathrm{On}$ such that $\kappa = \aleph_\alpha$. (iv) $\forall \alpha, \beta \in \mathrm{On}$, $\alpha < \beta$ implies $\aleph_\alpha < \aleph_\beta$. (v) $\aleph_\alpha$ is a successor cardinal if α is a successor ordinal, and is a limit cardinal if α is a limit ordinal.

Proof. (i), (ii) When α is a successor ordinal, (iv), and (v) are immediate from the definitions using Hartog's Lemma.

(ii) If λ is a limit ordinal we have that $\aleph_\lambda = \bigcup\{\aleph_\alpha^+ \mid \alpha < \lambda\}$ is a set by the axioms of replacement and unions, and so is an ordinal. And it is a cardinal because if $\gamma < \aleph_\lambda$ then there is $\alpha < \lambda$ such that $\gamma \in \aleph_\alpha^+ = \aleph_{s(\alpha)}$, and then $\overline{\overline{\gamma}} < \aleph_\alpha^+ < \aleph_\lambda$, and so $\gamma \not\sim \aleph_\lambda$.

(iii) Let $\kappa \in \mathrm{On}$ be an infinite cardinal. Then $\kappa = \{\gamma \in \mathrm{On} \mid \gamma < \kappa\} = \{\gamma \in \mathrm{On} \mid \gamma \preceq \kappa \,\&\, \kappa \not\preceq \gamma\} = \omega \cup \{\gamma \in \mathrm{On} \mid \exists \mu < \kappa\, \mu \text{ is a cardinal } \,\&\, \gamma \sim \mu\}$. So, if we have that for all cardinals $\mu < \kappa$ are alephs, then κ is an aleph. Thus any cardinal $\kappa \in \mathrm{On}$ is a aleph by the principle of induction on the ordinals.

Note. Without the axiom of choice is could be, for example, that $2^{\aleph_0}$ is not an ordinal.

4.3. Cardinals under AC.

Now we assume AC. So each cardinal can be well-ordered. Hence all cardinals are ordinals and the class of cardinals is well-ordered (and is a subclass of On).

Proposition. For all sets x, y, $x \preceq y$ if and only if $\overline{\overline{x}} \leq \overline{\overline{y}}$.

Proof. $x \preceq y$ if and only if $\overline{\overline{x}} \preceq \overline{\overline{y}}$. If $\overline{\overline{y}} < \overline{\overline{x}}$ we would have that $\overline{\overline{x}} \not\preceq \overline{\overline{y}}$. Thus $\overline{\overline{x}} \leq \overline{\overline{y}}$ by trichotomy.

Corollary. (AC) implies that for any x, y either there is an injection $i : x \longrightarrow y$, or there is an injection $j : y \longrightarrow x$.

Proof. Compare $\overline{\overline{x}}$ and $\overline{\overline{y}}$ in On.

Product theorem. (AC) Let κ be a cardinal. (Equivalently, let κ be an aleph.) Then $\kappa.\kappa = \kappa$.

Proof. First note that the Theorem is true for ω. If one defines $(k,l) \prec (m,n)$ if either $k+l < m+n$ or $k+l < m+n$ and $k < m$, or defines $(k,l) \prec' (m,n)$ if either $\max\{k,l\} < \max\{m,n\}$, or $\max\{k,l\} = \max\{m,n\}$ and $l < n$, or $\max\{k,l\} = \max\{m,n\}$, $l = n$ and $k < m$ it is clear that $\prec$ and $\prec'$ are well-orders of $\omega \times \omega$ and there are order-preserving bijections between them and $(\omega, \in)$.

Now we use induction. Suppose that the theorem is true for all infinite cardinals less than κ. Define an order on $\kappa \times \kappa$ by $(\alpha,\beta) \prec (\gamma,\delta)$ if $\alpha \cup \beta < \gamma \cup \delta$, or $\alpha \cup \beta = \gamma \cup \delta$ and $\beta < \delta$, or $\alpha \cup \beta = \gamma \cup \delta$, $\beta = \delta$ and $\alpha < \gamma$. Note that $\{(\alpha,\beta) \mid (\alpha,\beta) \preceq (\gamma,\gamma)\} = (\gamma+1) \times (\gamma+1)$ for any $\gamma < \kappa$

I claim that this order is a well-order. It is clear that $\prec$ is a partial order. and if $(\alpha,\beta) \not\prec (\gamma,\delta)$ and $(\gamma,\delta) \not\prec (\alpha,\beta)$ then $\alpha \cup \beta = \gamma \cup \delta$, $\beta = \delta$ and $\alpha = \gamma$, so $(\alpha,\beta) = (\gamma,\delta)$, and we have that $\prec$ is a total order. In order to see that $\prec$ is well-founded, let $Z \subseteq \kappa \times \kappa$ with $\emptyset \neq \emptyset$. Let ρ be minimal such that there is some $(\alpha,\beta) \in Z$ such that $\alpha \cup \beta = \rho$. Firstly let $Z_1 = \{(\alpha,\beta) \in Z \mid \alpha \cup \beta = \rho\}$. Let β_0 be minimal such that there is α with $(\alpha,\beta_0) \in Z_1$. Next let $Z_2 = \{(\alpha,\beta \in Z_1 \mid \beta = \beta_0\}$. Let α_0 be minimal such that $(\alpha_0,\beta_0) \in Z_2$. So (α_0,β_0) is $\prec$-minimal in Z.

Thus there is a unique $\rho \in$ On such that $(\kappa \times \kappa, \prec)$ is isomorphic to $(\rho, \in)$ via an order-preserving bijection. Let $f : (\rho, \in) \longrightarrow (\kappa \times \kappa, \prec)$ be the isomorphism. Suppose that $\kappa < \rho$ and that $f(\kappa) = (\alpha,\beta)$. Let $\gamma = \alpha \cup \beta$. Then $(\alpha,\beta) \preceq (\gamma,\gamma)$ and $f \restriction \kappa : \kappa \longrightarrow (\gamma+1) \times (\gamma+1)$ is an injection. Because κ is infinite we have that $\gamma \times \gamma$ is infinite, so γ is infinite. But $\gamma < \kappa$, then $\gamma+1 < \kappa$ and $\overline{\overline{\gamma+1}} < \kappa$. Thus, by the induction hypothesis. $\overline{\overline{s(\gamma)}}.\overline{\overline{s(\gamma)}} = \overline{\overline{s(\gamma)}}$. Hence $\kappa \prec s(\gamma) \times s(\gamma) \sim s(\gamma) \prec \kappa$. A contradiction! So $\rho = \kappa$.

Hence, by induction on the ordinals we have shown that $\kappa.\kappa = \kappa$ for all cardinals κ.

Corollary. Let κ be an infinite cardinal and let x_α be sets such that $\overline{\overline{x_\alpha}} \leq \kappa$ for all $\alpha < \kappa$. then $\bigcup\{x_\alpha \mid \alpha < \kappa\} \leq \kappa$.

Proof. We will apply AC to $Y = \{y_\alpha \mid \alpha < \kappa\}$, where for each $\alpha < \kappa$ we take

$$y_\alpha = \{f \mid f : x_\alpha \longrightarrow \kappa \text{ is an injection}\}.$$

Thus there is a function $g : Y \longrightarrow \bigcup Y$ such that $g_\alpha : x_\alpha \longrightarrow \kappa$ is an injection for each $\alpha < \kappa$. Define $h : \bigcup\{x_\alpha \mid \alpha < \kappa\} \longrightarrow \kappa \times \kappa$ by $h(z) = (\alpha, g_\alpha(z))$ where α is minimal such that $z \in x_\alpha$. Hence $\overline{\overline{\bigcup\{x_\alpha \mid \alpha < \kappa\}}} \leq \kappa$ by the Theorem.

Corollary. Let κ, μ be cardinals Suppose at least one of them is infinite (*i.e.*, an aleph).

(i) Then $\kappa + \mu = \max\{\kappa, \mu\}$.
(ii) Suppose neither κ or μ is equal to 0. Then $\kappa.\mu = \max\{\kappa, \mu\}$.
(iii) Suppose μ is infinite (an aleph) and $2 \leq \kappa \leq 2^\mu$. Then $\kappa^\mu = 2^\mu$.

Proof. (i) If $\kappa \leq \mu$, then $\mu \leq \kappa + \mu \leq \mu + \mu = 2.\mu \leq \mu.\mu = \mu$.
(ii) If $0 < \kappa < \mu$, then $\mu \leq \kappa.\mu \leq \mu.\mu = \mu$.
(iii) $2^\mu \leq \kappa^\mu \leq (2^\mu)^\mu = 2^{\mu.\mu} = 2^\mu$.

Corollary. $\aleph_\alpha + \aleph_\beta = \aleph_{\alpha\cup\beta} = \aleph_\alpha.\aleph_\beta$

Proof. $\aleph_{\alpha\cup\beta} = \aleph_{\max(\{\alpha\cup\beta\})} = \max(\{\aleph_\alpha, \aleph_\beta\})$.

Thus we have fixed + and . on cardinals. But expontiation is still a mystery, and it is here that the subject really starts to come to life. Cantor knew, as we have shown, that $\aleph_1 \leq 2^{\aleph_0}$ and, more generally, that $\aleph_{\alpha+1} \leq 2^{\aleph_\alpha}$ for each $\alpha \in \text{On}$, but could not show that there is any cardinal between any of these pairs. Thus he conjetured that, *the continuum hypothesis, (CH)*, that $\aleph_1 = 2^{\aleph_0}$ was true, and even that the *generalised continuum hypothesis (GCH)*, that $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$ for every ordinal α, was true. This is perhaps the simplest rule possible for cardinal exponentiation. But as we will see later *there is no reason to suppose that it is in fact true*. This is because it is not possible to show CH from ZFC (Cohen, 1963), nor to show that it is false(Gödel, 1938).

4.4. Cofinality.

Here we will see the sense in which GCH is a simple rule: it determines all the other rules of exponentiation. In order to do this we need a concept which is very useful quite apart from in studying exponentiation.

Definition. Let $\alpha, \beta \in \text{On}$ and let $f : \alpha \longrightarrow \beta$ be a function. f is *cofinal* (or *takes α cofinally (in)to β*) if $\forall\gamma < \beta\ \exists\delta < \alpha\ (\gamma \leq f(\delta))$.

Definition. Let $\beta \in \text{On}$. The *cofinality* of β, $\text{cf}\,(\beta)$, is the minimal α such that there is a cofinal function from α to β.

So, $\text{cf}\,(\beta) \leq \beta$ and is a cardinal for any β. And if β is a successor ordinal, then $\text{cf}\,(\beta) = 1$ (using the function $f(0) = \bigcup\beta$).

Proposition. There is a cofinal function $f : \text{cf}\,(\beta) \longrightarrow \beta$ which is strictly increasing ($\sigma < \tau < \text{cf}\,(\beta) \longrightarrow f(\sigma) < f(\tau)$), for any $\beta \in \text{On}$.

Proof. Let $g : \text{cf}\,(\beta) \longrightarrow \beta$ be any cofinal function, and define by recursion for $\tau < \text{cf}\,(\beta)$ the function $f(\tau) = \max(\{g(\tau), \sup\{f(\sigma) \mid \sigma < \tau\}\})$.

Proposition. If $\alpha \in \text{On}$ is a limit ordinal and $f : \alpha \longrightarrow \beta$ is cofinal and strictly increasing, then $\text{cf}\,(\alpha) = \text{cf}\,(\beta)$.

Proof. Let $g : \text{cf}\,(\alpha) \longrightarrow \alpha$ be any cofinal function. Then $f \cdot g : \text{cf}\,(\alpha) \longrightarrow \beta$ is cofinal. So $\text{cf}\,(\beta) \leq \text{cf}\,(\alpha)$. And if $h : \text{cf}\,(\beta) \longrightarrow \beta$ is cofinal, then $k : \text{cf}\,(\beta) \longrightarrow \alpha$ is cofinal, where $k(\tau) =$ the minimal σ such that $h(\tau) < f(\sigma)$.

Corollary. $\text{cf}\,(\text{cf}\,(\beta)) = \text{cf}\,(\beta)$ for any $\beta \in \text{On}$.

Proof. Immediate by the two previous propositions.

Corollary. Let α be a limit ordinal. Then $\text{cf}\,(\aleph_\alpha) = \text{cf}\,(\alpha)$.

Proof. Immediate by the last proposition using the $\aleph$-function.

Definition. Let $\beta \in \mathrm{On}$ be an infinite cardinal. If $\mathrm{cf}\,(\beta) = \beta$ we say that β is *regular*. If $\mathrm{cf}\,(\beta) < \beta$ we say that β is *singular*.

Examples. ω is regular. $\aleph_\omega$ is singular (See the second corollary to see that $\mathrm{cf}\,(\aleph_\omega) = \omega$).

Up to here nothing in this section has used AC.

Proposition. (AC) implies κ^+ is regular for any cardinal κ.

Proof. If $f : \alpha \longrightarrow \kappa^+$ is cofinal where $\alpha < \kappa^+$, then $\kappa^+ = \bigcup\{\, f(\gamma) \mid \gamma < \alpha\}$. But $f(\gamma)$, $\alpha < \kappa$, so $\overline{\overline{f(\gamma)}}$, $\overline{\overline{\alpha}} < \kappa^+$ and we would have that κ^+ would be a union of κ sets each with cardinality $\leq \kappa$. A contradiction to the first Corollary to the Product Theorem of §4.3.

(**Note.** Without (AC) it is possible that $\mathrm{cf}\,(\omega_1) = \omega$.)

A natural question now is whether there limit cardinals that are also regular. If $\aleph_\alpha$ is such a cardinal, then $\aleph_\alpha = \alpha$. But this alone is not enough. For example, if $\alpha = \bigcup\{\,\aleph_0, \aleph_\omega, \aleph_{\omega_\omega}, \ldots\}$ we have that $\aleph_\alpha = \alpha$ but $\mathrm{cf}\,(\alpha) = \omega$. Thus the first cardinal that is both a limit cardinal and regular (if such exists) is bigger than this.

Definition. κ is *weakly inacessible* if it is both a limit cardinal and is regular.

Definition. (AC) κ is *strongly inacessible* if it is regular and $\forall \mu < \kappa\, 2^\mu < \kappa$.

Proposition. If κ is strongly inacessible it is weakly inaccessible. And (GCH) implies that if κ is weakly inacessible, it is strongly inacessible.

Now we use the notion of cofinality to help show how (GCH) simplifies cardinal exponentiation.

Proposition. Let κ be an infinite cardinal and $\mathrm{cf}\,(\kappa) \leq \mu$. Then $\kappa^\mu \not\preceq^* \kappa$.

Proof. The proof is a variant of Cantor's proof that $\mathcal{P}(x) \not\preceq^* x$ that we saw in §1.1. Let $f : \mu \longrightarrow \kappa$ be any cofinal function and let $g : \kappa \longrightarrow {}^\mu\kappa$ be any function. We shall show that g cannot be a surjection. Define $h : \mu \longrightarrow \kappa$ by setting $h(\alpha) =$ the minimal element of $\kappa \setminus \{\,(g(\beta))(\alpha) \mid \beta < f(\alpha)\}$. If $\gamma < \kappa$ one can choose $\alpha < \mu$ such that $\gamma < f(\alpha)$ because f is cofinal. So we have $h(\alpha) \neq g(\gamma)(\alpha)$. Hence $h(\alpha) \notin \mathrm{im}(g)$.

Corollary. (AC) Let κ be an infinite cardinal and $\mathrm{cf}\,(\kappa) \leq \mu$. Then $\kappa < \kappa^\mu$.

Proof. It is clear that $\kappa \preceq \kappa^\mu$, hence by the proposition and trichotomy $\kappa < \kappa^\mu$.

Corollary. (AC) Let κ be an infinite cardinal, then $\kappa < \mathrm{cf}\,(2^\kappa)$.

Proof. If $\mathrm{cf}\,(2^\kappa) \leq \kappa$ we have that $2^\kappa < (2^\kappa)^\kappa = 2^{\kappa.\kappa} = 2^\kappa$, a contradiction.

Proposition. (AC + GCH) Let κ, μ be cardinals, $2 \leq \kappa$, μ infinite. then, (i) $\kappa \leq \mu \longrightarrow \kappa^\mu = \mu^+$, (ii) $\mathrm{cf}\,(\kappa) \leq \mu < \kappa \longrightarrow \kappa^\mu = \kappa^+$, and (iii) $\mu < \mathrm{cf}\,(\kappa) \longrightarrow \kappa^\mu = \kappa$,

Proof. (i) We have already seen (without GCH) that $\kappa^\mu = 2^\mu$. (GCH) says that $2^\mu = \mu^+$.
(ii) The first corollary above says $\kappa < \kappa^\mu$. But $\kappa^\mu \leq \kappa^\kappa = 2^\kappa, = \kappa^+$ by (GCH).
(iii) $\mu < \mathrm{cf}\,(\kappa)$ says that any function $f : \mu \longrightarrow \kappa$ is not cofinal. Thus ${}^\mu\kappa = \bigcup\{\,{}^\mu\alpha \mid \alpha < \kappa\}$, and $\overline{\overline{{}^\mu\alpha}} \leq \max(\{\overline{\overline{\alpha}}, \mu\})^+ \leq \kappa$.

Without (GCH) exponentiation can be much more complicated. There are many things that are independent of ZFC – *i.e.*, they cannot be proved but neither can their contraries. (See the remainder of the course for more explanation of this.) However there *are* some results that can be shown in ZFC, and various important questions are open. For example we have the following.

Theorem. (Silver, 1975) If $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ for all $\alpha < \omega_1$, then $2^{\aleph_{\omega_1}} = \aleph_{\omega_1+1}$

And we have similar results for other cardinals κ with $\omega < \mathrm{cf}\,(\kappa) < \kappa$.

Thus one can forulate the *Singular Cardinals Hypothesis* in analogy to the GCH. The SCH is that if κ is singular and $\mathrm{cf}\,(\kappa) = \mu$ then $\kappa^\mu = \min\{\kappa^+, 2^\mu\}$.

However, in contrast to Silver's Theorem (and to what is envisaged by SCH), the situation is very different – and even more complicated – for singular cardinals κ with $\mathrm{cf}\,(\kappa) = \omega$, as the following two theorems illustrate.

First a theorem which talks about the freedom that one has:

Theorem. (Gitik-Magidor, 1989) For any $\delta < \omega_1$ and it is possible that $2^{\aleph_n} = \aleph_{n+1}$ for all $n < \omega$, but $2^{\aleph_\omega} = \aleph_{\delta+1}$.

And next a theorem that shows that there are nevertheless some limitations when $\mathrm{cf}\,(\kappa) = \omega$.

Theorem. (Shelah, 1989) If $2^{\alpha_n} < \aleph_\omega$ for each $n < \omega$, then $2^{\aleph_\omega} < \min(\{\aleph_{\omega_4}, \aleph_{(2^\omega)^+}\})$.

One of the outstanding open questions in this part of set theory is whether the "4" in Shelah's Theorem above can be improved. (Perhaps to "1" although any improvement would be very significant.)