3.1.3. Tétel. *Tekintsük $\mathbb{N} \times \mathbb{N}$-en az $(m,n) \sim (m',n')$, ha $m+n' = m'+n$ relációt és az $(m,n)+(m',n') = (m+m', n+n')$ összeadást. A $\sim$ reláció ekvivalenciareláció. Az ekvivalenciosztályok halmazát $\mathbb{Z}$-vel fogjuk jelölni, és elemeit* egész számok*nak nevezzük. Az összeadás kompatibilis az ekvivalenciával, így az egész számok között értelmezve van az összeadás és $\mathbb{Z}$ az összeadásra nézve Abel-csoport.*

Bizonyítás. A $\sim$ reláció nyilván ekvivalenciareláció (az összeadás kommutativitását, asszociativitását és a természetes számok összeadásának egyszerűsítési szabályát használjuk fel a bizonyításhoz).

Megmutatjuk, hogy a párok összeadása kompatibilis az ekvivalenciarelációval. Mivel a párok összeadása kommutatív, elég azt megmutatni, hogy ha $(m,n) \sim (m',n')$, akkor $(m,n) + (m'',n'') \sim (m',n') + (m'',n'')$. Az, hogy $(m,n) \sim (m',n')$, azt jelenti, hogy $m + n' = m' + n$. Ebből $m + m'' + n' + n'' = n + n'' + m' + m''$, ami viszont azt jelenti, hogy

$$(m,n) + (m'',n'') = (m + m'', n + n'') \sim (m' + m'', n' + n'') = (m',n') + (m'',n'').$$

Mivel a párok összeadása kommutatív és asszociatív, az ekvivalenciosztályoké is. A $(0,0)$ pár osztálya nullelem, ezt jelöljük nullával. Az (m,n) pár osztályának additív inverze az (n,m) pár osztálya. Így $\mathbb{Z}$ az összeadással Abel-csoport.

3.1.4. Tétel: $\mathbb{N}$ beágyazása $\mathbb{Z}$-be. *Az előző tétel jelöléseivel, a $\varphi : n \mapsto \widetilde{(n,0)}$ leképezése $\mathbb{N}$-nek $\mathbb{Z}$-be kölcsönösen egyértelmű, összeadástartó, valamint $\varphi(n) = n\varphi(1)$ minden $n \in \mathbb{N}$-re. Így $\varphi(\mathbb{N})$-et azonosíthatjuk $\mathbb{N}$-el. Ezzel az azonosítással $\mathbb{N} \cup (-\mathbb{N}) = \mathbb{Z}$ és $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$.*

Bizonyítás. Mivel megállapodás szerint, ha semmit sem adunk össze, az összeg a nullelem, $0\varphi(1) = \widetilde{(0,0)} = \varphi(0)$. Ugyancsak az összeg definíciója szerint $1\varphi(1) = \widetilde{(1,0)} = \varphi(1)$. Teljes indukcióval

$$\varphi(n^+) = n\varphi(1) + \varphi(1) = \widetilde{(n,0)} + \widetilde{(1,0)} = \widetilde{(n+1,0)} = \varphi(n^+)$$

minden $n \in \mathbb{N}$-re. Az állítás többi része adódik, ha belátjuk, hogy $\mathbb{Z}$ minden eleme, azaz minden ekvivalenciaosztály pontosan egyet tartalmaz a $(k,0)$ illetve $(0,k)$ alakú elemek közül, ahol $k \in \mathbb{N}$. Legyen $m,n \in \mathbb{N}$. Ha $n \geq m$, akkor van olyan $k \in \mathbb{N}$, amelyre $n = m + k$; ekkor $(m,n) \sim (k,0)$. Hasonlóan, ha $n \leq m$, akkor van olyan $k \in \mathbb{N}$, hogy $n + k = m$; ekkor $(m,n) \sim (0,k)$. Másrészt, ha $(k,0) \sim (k',0)$, akkor $k = k'$; ha $(0,k) \sim (0,k')$, akkor is $k = k'$; végül ha $(k,0) \sim (0,k')$, akkor $k = k' = 0$. $\square$

3.1.5. Az egész számok rendezése. Ha $m,n \in \mathbb{Z}$, akkor legyen $m \leq n$, ha van olyan $k \in \mathbb{N}$, amelyre $m + k = n$. Ez persze ugyanazt jelenti, mint hogy $n - m \in \mathbb{N}$. Ugyanúgy, mint a természetes számoknál, adódik, hogy így egy részbenrendezést kapunk. Az egész számok körében $-\mathbb{N}$ elemeit az jellemzi, hogy kisebb vagy egyenlőek, mint nulla: ha $n \in \mathbb{N}$, akkor $(-n) + n = 0$, így $-n \leq 0$, és ha $m \leq 0$, akkor valamely $n \in \mathbb{N}$-re $m + n = 0$, azaz $m = -n$. Innen következik, hogy $-\mathbb{N}$ bármely eleme kisebb vagy egyenlő, mint $\mathbb{N}$ bármely eleme. Mivel $m \leq n$ esetén $n - m \in \mathbb{N}$, azt kapjuk, hogy

$(-n) + (n - m) = -m$, azaz $-\mathbb{N}$ elemei is összehasolíthatóak. Ezzel beláttuk, hogy $\mathbb{Z}$ rendezett. Megmutatjuk, hogy ha $k, m, n \in \mathbb{Z}$ és $m \leq n$, akkor $m + k \leq n + k$; valóban, $(n + k) - (m + k) = n - m \in \mathbb{N}$. Ezt a tulajdonságot úgy hívjuk, hogy az *összeadás monoton*.

3.1.6. Az egész számok szorzása. Ha $m, n \in \mathbb{Z}$, akkor az $m, n \in \mathbb{N}$ esetben legyen mn a természetes számokra definiált szorzat, ha $m, -n \in \mathbb{N}$, akkor legyen $mn = nm = -m(-n)$, és ha $-m, -n \in \mathbb{N}$, akkor legyen $mn = (-m)(-n)$. Esetszétválasztással azonnal adódik, hogy a szorzat pontosan akkor lesz nulla, ha valamelyik tényezője nulla, ezzel a szorzással $\mathbb{Z}$ kommutatív félcsoport az 1 egységelemmel, valamint ha $k, m, n \in \mathbb{Z}$, akkor $k \cdot (m + n) = k \cdot m + k \cdot n$, azaz a szorzás *disztributív* az összeadásra nézve. (Rövidesen belátjuk az úgynevezett előjelszabályt, amelyből következik, hogy a szorzást nem is definiálhattuk volna másként, ha azt akarjuk, hogy disztributív legyen az összeadásra nézve.)

3.1.7. Hatványozás egész kitevővel. Ha G egy csoport, $g \in G$, akkor az $n \mapsto g^n$ leképezést a $g^{-n} = (g^{-1})^n$, ha $n \in \mathbb{N}^+$ definícióval kiterjeszthetjük egy $\mathbb{Z}$-n értelmezett leképezéssé.

Mint esetszétválasztással nem nehéz belátni, erre a leképezésre $g^{m+n} = g^m g^n$ és $(g^m)^n = g^{mn}$ minden $m, n \in \mathbb{Z}$-re, továbbá ha $g, h \in G$ felcserélhető elemek, akkor $(gh)^n = g^n h^n$ minden $n \in \mathbb{Z}$-re.

Ha G Abel-csoport additív írásmóddal, akkor g^n helyett ng-t írunk. Figyelem, $(n, g) \mapsto ng$, $g \in G$, $n \in \mathbb{Z}$ nem művelet, hanem ismételt összeadással van definiálva! A fenti összefüggések ezzel a jelöléssel $(m + n)g = mg + ng$, $m(ng) = (mn)g$ és $n(g + h) = ng + nh$ minden $m, n \in \mathbb{Z}$, $g, h \in G$ esetén.

3.1.8. Gyűrűk. Egy R halmazt egy $(+, \cdot)$ binér műveletekből álló párral *gyűrű*nek nevezünk, ha az összeadással Abel-csoport (a nullelemet 0 fogja jelölni), a szorzással félcsoport, és teljesül mindkét oldali disztributivitás, azaz ha $x, y, z \in R$, akkor

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{és} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Ha a szorzás kommutatív, akkor a gyűrűt *kommutatív gyűrű*nek nevezzük. Ha a szorzásnak van egységeleme, akkor a gyűrűt *egységelemes gyűrű*nek nevezzük.

Tetszőleges gyűrűben $x0 = x(0 + 0) = x0 + x0$. Mindkét oldalhoz hozzáadva $-x0$-t, kapjuk, hogy $x0 = 0$. Hasonlóan adódik, hogy $0x = 0$. Érvényes az úgynevezett „előjelszabály” is: $(-x)y = x(-y) = -xy$ és $(-x)(-y) = xy$ minden x, y elemre. Például $xy + (-x)y = \big(x + (-x)\big)y = 0y = 0$, amiből az inverz egyértelműsége miatt $(-x)y = -xy$; a többi összefüggés hasonlóan adódik. Az is teljesül, hogy $n(xy) = (nx)y = x(ny)$ minden x, y gyűrűbeli elemre és $n \in \mathbb{Z}$-re. (Figyelem, $(n, x) \mapsto nx$ nem a gyűrűbeli szorzás, hanem ismételt összeadással van definiálva!) Ha $n \in \mathbb{N}$, ekkor ez az összefüggés teljes indukcióval adódik, felhasználva a disztributivitást; innen az általános esetet az előjelszabály felhasználásával kapjuk.

A legegyszerűbb példa a *nullgyűrű*, amely csak egy elemet tartalmaz, ez nyilván a 0. Másik triviális példa egy (additív) Abel-csoport, amelyben bármely két elem szorzatát nullának értelmezzük; ezeket a gyűrűket *zérógyűrű*nek nevezzük. Fontosabb példa $\mathbb{Z}$. Ezek a gyűrűk mind kommutatív gyűrűk, a nullgyűrű és $\mathbb{Z}$ egységelemesek.