3

Def G groep. $H \subset G$. Dan heet H een ondergroep van G als:

(H0) $H \neq \emptyset$

(H1) $\forall a,b \in H: \; ab \in H$

(H2) $\forall a \in H: \; a^{-1} \in H$, waarbij a^{-1} de inverse van a onder $\circ: G \times G \to G$ is.

St 3.3 G groep $H \subseteq G$ ondergroep, dan beperkt $\circ: G \times G \to G$ tot H en is H met $\circ|_H : H \times H \to H$ zelf een groep.

Bewijs omdat H gesloten is onder de groepswet $\circ$ via (H1), geldt dat als $(a,b) \in H \times H$, dat $a \circ b \in H$, dus we kunnen $\circ$ beperken tot H. Onder $\circ|_H$ blijkt dat in H aan (G1) voldaan is, want $a,b,c \in H \overset{(H \subseteq G)}{\Rightarrow} a,b,c \in G \overset{(G1 \text{ op } G)}{\Rightarrow} a(bc) = (ab)c$, klaar.
Omdat $H \neq \emptyset$ geldt $\exists x: x \in H$, en dan via (H2) $x^{-1} \in H$, dus $x \circ|_H x^{-1} = x \circ x^{-1} = e \in H$ via (H1), en $\forall x \in H$: omdat $e \circ x = x = x \circ e$ als $x \in G$ en $H \subset G$, geldt (G2)
(G3) is precies (H2), omdat x^{-1} ook de inverse van x is onder $\circ|H$ ■

St. 3.4 $H \subseteq G$, G groep dan is H o.g. desda
(H0) $H \neq \emptyset$
(H1') $\forall a,b \in H: \; ab^{-1} \in H$.

Vb $H = \{e\}$ en $H = G$ zijn altijd ondergroepen van G. We noemen deze triviaal

St. 3.5 Zij $(H_i)_{i \in I}$ een collectie van o.g. van G, dwz H_i o.g. v G voor alle $i \in I$. Dan $\bigcap_{i \in I} H_i$ ook o.g. van G.

St. 3.6 (a) Elke o.g. van $\mathbb{Z}$ is van de vorm $m\mathbb{Z} := \{mz \in \mathbb{Z} \mid z \in \mathbb{Z}\}$ met $m \in \mathbb{Z}_{\geq 0}$
Elke $m\mathbb{Z}$ is ook een ondergroep van $\mathbb{Z}$.

(b)* Elke o.g. H van $\mathbb{Z}/n\mathbb{Z}$ voor $n \in \mathbb{Z}_{\geq 0}$ is van de vorm: $\exists d^{>0}$ deelt n en $H = \{\overline{ad} \in \mathbb{Z}/n\mathbb{Z} \mid a \in \{1, .., \frac{n}{d}\}\} = d\mathbb{Z}/n\mathbb{Z}$

* Opm. (b) volgt ook uit (a) en de later bewezen stelling dat elke o.g. van G/N voor $N \lhd G$ van de vorm H/N is met H o.g van G en $N \subset H$

Bew. (a) Zij $H \subseteq \mathbb{Z}$ o.g. Als $H = \{0\}$, dus triviaal, dan $H = 0\mathbb{Z}$.
als $H \neq \{0\}$, dan is er een niet-nulelement $a \in H$ en
als $a < 0$ dan ook $-a \in H$, dus er is een $a \in H$ zdd
$a > 0$. Zij dus m het kleinste positieve element in H.
Bewering: $H = m\mathbb{Z}$. Bewijs:
"$\supseteq$" omdat $m \in \mathbb{Z}$ geldt $\overset{m \cdot 1 =}{1m} \in H$. voor elke $n \in \mathbb{Z}_{\geq 0}$
geldt nu $mn \in H$ met inductie naar n:
IB $n = 0$: $0 \in H$ want 0 is eenheid, dus $m \cdot 0 \in H$
IS stel $m(n-1) \in H$, dan omdat $m \in H$ geldt $m + m(n-1) = mn \in H$
$\square$
Omdat ook $-x \in H$ voor elke $x \in H$, geldt ook voor $x \in \mathbb{Z}_{<0}$
dat $mx = \underbrace{-m(-x)}_{\in H} \in H$. Dus $m\mathbb{Z} \subset H$
"$\subseteq$" Stel $x \in H$
en neem $x = qm + r$, deling met rest dus $0 \leq r < m$
als $r \neq 0$, dan is er een kleiner positief element, namelijk
$r \in H$ dan m, in tegenspraak met de aanname. Dus $r = 0$
waardoor deelt m x, dus $x = qm$, $q \in \mathbb{Z}$, dus
$x \in m\mathbb{Z}$
uit "$\supset$" en "$\subset$" volgt $H = m\mathbb{Z}$

(opm dit bewijs is ook te lezen als bewijs voor meer alg. G/N)

(b) Zij $H \subset \mathbb{Z}/n\mathbb{Z}$ ondergroep.
Definieer $K \subset \mathbb{Z}$ door $K := \{a \in \mathbb{Z} \mid \bar{a} \in H\}$
$\bar{0} \in H$, want H is o.g., dus $0 \in K$ $\Rightarrow$ (H0)
als $a, b \in K$ dan $\bar{a}, \bar{b} \in H$, dus $\overline{a-b} \in H$, dus $a - b \in K$ $\Rightarrow$ (H1')
Hieruit blijkt dat K een o.g. van $\mathbb{Z}$ is, dus via (a):
$K = d\mathbb{Z}$ voor $d \in \mathbb{Z}_{>0}$. Omdat $\bar{0} = \bar{n}$ en dus $n \in K = d\mathbb{Z}$,
geldt d deelt n. Daardoor
$$H = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid a \in K\} = \{\ldots, \overline{-3d}, \overline{-2d}, \ldots\}$$
$$= \{\bar{d}, \overline{2d}, \ldots \bar{n}\} = \{\overline{md} \in \mathbb{Z}/n\mathbb{Z} \mid m \in \{1, \ldots, \tfrac{n}{d}\}\}$$
$\blacksquare$

Def 3.7 G_1 G_2 groepen. $f: G_1 \to G_2$ heet een (groeps)homomorfisme
als $\forall x, y \in G_1$: $f(x)f(y) = f(xy)$

Def's een isomorfisme is een bijectief homomorfisme
een endomorfisme is een homomorfisme $G \to G$
een automorfisme is een bijectief endomorfisme.
(een inwendig automorfisme is een automorfisme dat van de vorm $x \mapsto axa^{-1}$ is voor een vaste $a \in G$)

St. 3.10 $f(e_1) = e_2$; $f(a^{-1}) = f(a)^{-1}$

Def $\mathrm{Ker}(f) := \{x \in G_1 \mid f(x) = e_2\}$, de kern van f.

$\mathrm{Im}(f) := \{x_2 \in G_2 \mid \exists x_1 \in G_1 : f(x_1) = x_2\} = f(G_1)$

St. 3.13 $f: G_1 \to G_2$ homom. dan is $\mathrm{Ker}(f)$ een o.g. van G_1 en is $\mathrm{Im}(f)$ een o.g. van G_2. Echter niet elke o.g. is een kern van een homom. !
(wel elke normaaldeler)

St 3.14 $f: G_1 \to G_2$ homom : f injectief desda $\mathrm{Ker}(f) = e$.

St. 3.17 samenstellingen van homom's zijn homom's $f: G_1 \to G_2$, $g\, G_2 \to G_3$: $f \circ g : G_1 \to G_3$
samenstellingen van isomorfismen zijn isomorfismen.

3.18 als f isomorfisme is, dan f^{-1} (bestaat, f is bijectief dus inverteerbaar) ook een isomorfisme.

Bewijs 3.18 $f(f^{-1}(xy)) = xy = f(f^{-1}(x))\, f(f^{-1}(y)) \overset{f \text{ homom.}}{=} f(f^{-1}(x)\, f^{-1}(y))$
pas nu op de gelijkheid f^{-1} toe, dan
$$f^{-1}(xy) = f^{-1}(f(f^{-1}(xy))) = f^{-1}(f(f^{-1}(x) f^{-1}(y))) = f^{-1}(x) f^{-1}(y)$$
■

Def als er een isomorfisme $f: G_1 \to G_2$ is $G_1\ G_2$ groepen, dan noemen we G_1 isomorf met G_2, notatie $G_1 \cong G_2$

Lemma Dit is een equivalentie relatie $\begin{cases} G_1 \cong G_2 \Rightarrow G_2 \cong G_1 \\ G_1 \cong G_2 \quad G_2 \cong G_3 \Rightarrow G_1 \cong G_3 \\ G_1 \cong G_1 \quad \forall G_1 \text{ groep.} \end{cases}$

Def 3.20 Voor G_1, G_2 groepen definieert men het directe product $G_1 \times G_2$ als de verzameling het carthesisch product van G_1 met G_2, dus $\{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$
en met de bewerking $* : (G_1 \times G_2) \times (G_1 \times G_2) \to (G_1 \times G_2)$
gegeven door $(a,b) * (c,d) := (a \circ c, b \bullet d)$ waarbij $\circ, \bullet$ de groepnwet op G_1 resp. G_2 zijn

St. het directe product is met $*$ een groep, met eenheid $e = (e_1, e_2)$ en inverse $\underset{(G_1 \times G_2)}{\underset{\cap}{(x,y)}}^{-1} = (\underset{G_1}{\underset{\cap}{x^{-1}}}, \underset{G_2}{\underset{\cap}{y^{-1}}})$

St. als H_1, H_2 o.g. van G zijn zdd
(a) $h_2 h_1 = h_1 h_2 \quad \forall h_1 \in H_1, h_2 \in H_2$
(b) $H_1 \cap H_2 = \{e\}$
(c) elke $\forall g \in G : g = h_1 h_2, \exists h_1 \in H_1 \exists h_2 \in H_2$

Dan $G \cong H_1 \times H_2$ door isomorfisme $(h_1, h_2) \mapsto h_1 h_2$
Bewijs: ga na dat dit isomorfisme is.

St. 3.25 (Chinese reststelling) $n, m \in \mathbb{Z}_{>0}$, $\text{ggd}(n,m) = 1$, dan is er een isomorfisme $\mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$
door $(a \bmod mn) \longmapsto ((a \bmod n), (a \bmod m))$

Bew met $f : (a \bmod mn) \mapsto ((a \bmod n), (a \bmod m))$
is f allereerst welgedefinieerd en homomorf.

Lemma $f : (\mathbb{Z}/m\mathbb{Z}) \to (\mathbb{Z}/d\mathbb{Z})$ met $d \mid m$ door $(a \bmod m) \mapsto (a \bmod d)$ is een welgedefinieerd homom.
Bewijs: $(a \bmod m) = (b \bmod m)$, dan $a - b \in m\mathbb{Z} \subset d\mathbb{Z}$
dus $a - b \in d\mathbb{Z} \Rightarrow (a \bmod d) = (b \bmod d)$
en $f((a \bmod m) + (b \bmod m)) = f((a + b \bmod m)) = (a + b \bmod d)$
$= (a \bmod d) + (b \bmod d) = f((a \bmod m)) + f((b \bmod m))$ ■

als $a \equiv b \bmod mn$, dan aangezien $n \mid nm$, $m \mid nm$:
dan $f((a \bmod mn)) = ((a \bmod n), (a \bmod m)) = ((b \bmod n), (b \bmod m))$
$= f((b \bmod mn))$ en $f(\bar{a} + \bar{b}) = (\widehat{a + b}, \widetilde{a + b}) = (\hat{a} + \hat{b}, \tilde{a} + \tilde{b})$
$= (\hat{a}, \tilde{a}) + (\hat{b}, \tilde{b}) = f(\bar{a}) + f(\bar{b})$

bovendien is f injectief, want $\bar{a} \in Ker(f) \Leftrightarrow f(\bar{a}) = (\hat{0}, \tilde{0})$
$\Leftrightarrow a \equiv 0 \mod m, \; a \equiv 0 \mod n \Leftrightarrow m|a, \; n|a \Leftrightarrow kgv(m,n)|a$
maar $kgv(m,n) = mn$ want $ggd(m,n) = 1$, dus $\Leftrightarrow mn|a \Leftrightarrow$
$a \equiv 0 \mod mn \Leftrightarrow \bar{a} = \bar{0}$. dus $Ker(f) = \{\bar{0}\}$

Nu geldt altijd $im(f) \subseteq (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$
en omdat f injectief en $\#(\mathbb{Z}/nm\mathbb{Z}) = nm < \infty$ is,
geldt $\# im(f) = \#(\mathbb{Z}/mn\mathbb{Z}) = mn$, maar $\#((\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})) = nm$,
dus $im(f) = (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \Rightarrow f$ surjectief. dus f is isomorfisme □

3.26 (Chinese Reststelling) $n, m \in \mathbb{Z}_{>0}$, $ggd(n,m) = 1$.
Dan is er een $a \in \mathbb{Z}$ zdd $\begin{cases} a \equiv b \mod n \\ a \equiv c \mod m \end{cases}$

en deze a is modulo mn uniek bepaald, dus in $\mathbb{Z}/nm\mathbb{Z}$ is $\bar{a}$ uniek.
Dit is een alternatieve formulering, die zegt dat f uit st. 3.25 een inverteerbare functie is die homomorf is, dus dat f een isomorfisme is.

* Rekenvoorbeeld: methode is om met Euclidisch Algoritme $x, y \in \mathbb{Z}$ te vinden zdd $xn + ym = 1$ (dat kan via 1.9)
vervolgens vinden we $bym \equiv b \mod n$, $cxn \equiv c \mod m$
dus $bym + cxn$ voldoet aan het stelsel.

$30 = 4 \cdot 7 + 2 = 1 \cdot 30 + 0 \cdot 7$

$\begin{cases} a \equiv 27 \mod 30 \\ a \equiv 5 \mod 7 \end{cases} \Rightarrow$ $7 = 3 \cdot 2 + 1 = 0 \cdot 30 + 1 \cdot 7$

$2 = 2 \cdot 1 + 0 = 1 \cdot 30 - 4 \cdot 7$

$1 = \text{———} = -3 \cdot 30 + 13 \cdot 7$

dus $a \equiv -3 \cdot 30 \cdot 5 + 13 \cdot 7 \cdot 27 \mod 210 \equiv 117 \mod 210$

3.27 Herhaald toepassen van het homomorfisme geeft inductief
voor $n_1, \dots, n_t \in \mathbb{Z}_{>0}$ $ggd(n_i, n_j) = 1$ voor $i \neq j$, dan met $N = \prod_{i=1}^{t} n_i$
$(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\dots) \times (\mathbb{Z}/n_t\mathbb{Z})$

Zo'n stelsel is op te lossen door steeds 2 vgl. te nemen en hierop methode * toe te passen, vervolgens verder te rekenen met $\begin{cases} a \equiv b \mod m \\ a \equiv c \mod n \end{cases}$ vervangen door $a \equiv s \mod mn$