1 Theorie

1. Geef en bewijs de structuurstelling.
2. Alice wil een boodschap doorgeven aan Bob door gebruik te maken van het RSA systeem. Hoe doet ze dat? Hoe ontcijfert Bob het bericht? *Bijvraag:* Uitleg geven bij hetgene je hebt opgeschreven en vragen beantwoorden in de trand van: bewijs dat de methode die Bob gebruikt om te ontcijferen daadwerkelijk werkt en hoe bereken je $C^d \mod n$ efficiënt?

2 Oefeningen

1. Zij $G, \cdot$ een groep en H een deelgroep van G. We definiëren de normalisator van H als de deelverzameling
$$N(H) := \{g \in G | gH = Hg\}$$
   (a) Toon aan dat $N(H)$ een deelgroep is van G die H omvat.
   (b) Geef een voorbeeld van een groep $G, \cdot$ en een niet-triviale deelgroep H zodat $N(H) = H$.
   (c) Geef een voorbeeld van een groep $G, \cdot$ en een niet-triviale deelgroep H zodat $N(H) \neq H$.
   (d) Stel $x \in G$. Toon aan dat $N(xHx^{-1}) = xN(H)x^{-1}$
2. Bepaal alle $x \in \mathbb{Z}$ zodat $2019x \equiv 18^{2019} \mod 45$
3. Zij K een veld en zij V een eindigdimensionale K-vectorruimte. Beschouw een billinieaire vorm $\langle \cdot, \cdot \rangle$ op V en definieer de volgende afbeeldingen:
$$L : V \to V^* : v \longmapsto \langle v, - \rangle$$
$$R : V \to V^* : v \longmapsto \langle -, v \rangle$$
   (a) Zij $\phi : V \to V^{**} : v \longmapsto \mathrm{ev}_v$ het kanonieke isomorfisme. Toon aan dat $L^* \circ \phi = R$ en $R^* \circ \phi = L$.
   (b) Zij $\mathcal{V} = \{v_1, v_2, ..., v_n\}$ een basis van V en zij $\mathcal{V}^*$ zijn duale basis. Toon aan dat de gram-matrix van de gegeven billinieaire vorm tov $\mathcal{V}$ gelijk is aan de matrix van R ten opzichte van $\mathcal{V}$ en $\mathcal{V}^*$. Bepaal ook de matrix van L ten opzichte van $\mathcal{V}$ en $\mathcal{V}^*$ in functie van de gram-matrix.
   (c) Toon aan dat elke $l \in V^*$ van de vorm $\langle v, - \rangle$ is voor een unieke $v \in V$ als en slechts als de billineaire vorm niet-ontaard is.