

Algebra I (2010)

Harjoitus 5/viikko 48

- (1) Olkoon $A = \{a, c, \dots, y, z\}$ ja käytetään vastaavuutta $a \leftrightarrow 1, b \leftrightarrow 2, \dots, z \leftrightarrow 26$. Koodataan 2-pituiset merkkijonot 32-järjestelmän luvuiksi; esim. $bc \mapsto 2 \cdot 32 + 3$. Olkoon julkinen salausavain $(e, m) = (11, 10403)$. Murra salattu viesti 1450.
- (2) Etsi kaikki jaottomat astetta neljä olevat \mathbb{F}_2 -kertoimiset polynomit.
- (3) Olkoon G syklinen ryhmä ja H sen aliryhmä.
 - (a) Osoita, että H on syklinen.
 - (b) Oletetaan, että $G = \langle g \rangle$, $|G| = n$. Todista:
 - (i) $g^i = g^j \Leftrightarrow i \equiv j \pmod{n}$.
 - (ii) Jokaista luvun n tekijää d kohti on täsmälleen yksi kertalukua d oleva G :n aliryhmä H .
- (4)
 - (a) Etsi kaikki ryhmän (\mathbb{R}^*, \cdot) äärelliset aliryhmät.
 - (b) Etsi kaikki ryhmän $(\mathbb{Z}, +)$ aliryhmät.
- (5)
 - (a) Olkoon K kunta ja $f \in K[x]$. Osoita, että polynomilla f on korkeintaan $\deg f$ nollakohtaa kunnassa K .
 - (b) Osoita, että äärellisen kunnan \mathbb{F} kertolaskuryhmä \mathbb{F}^* on syklinen.
- (6)
 - (a) Etsi jokin ryhmän \mathbb{F}_{16}^* generoija kun $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$, missä $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$.
 - (b) Etsi kaikki ryhmän \mathbb{F}_{16}^* aliryhmät.