Lõplikud korpused I

Kordamisküsimused

Sügis 2019

Eksamipilet koosneb ühest kuni kahest teoreemist ja kahest ülesandest.

Teoreemid tuleb sõnastada ja tõestada ning need valitakse alljärgnevast nimekirjast. Kasutatud lühendid: L&N – Lidl&Niederreiter, 2nd ed., 1997. Tõestused ei pea olema põhjalikumad, kui algmaterjalis, st. varasematele tulemustele võib ilma tõestuseta viidata, nt. L&N Teoreem 1.86 toetub tulemustele L&N 1.40, 1.61, 1.82, 1.85 ja Eukleidese algoritmile, millele võib siis (need omakorda sõnastades!) viidata. Erandiks on siin väga skemaatiline L&N teoreem 1.91, mida tuleb käsitleda loenguga samal detailsusastmel.

Eksami ajal on lubatud kasutada abimaterjale kuni 3 minuti vältel, millele lisanduvad TEX-lisaminutid. Enne abimaterjalide kasutamist tuleb ära anda definitsioonid ja sõnastused, hilisemat võetakse arvesse ainult tõestuse osa hindamisel.

1. Tsükliliste rühmade omadusi (L&N 1.15),
2. Rühmade klassivõrrand (L&N 1.27),
3. Teoreem kommutatiivse ringi faktorringi struktuurist (L&N 1.47),
4. Teoreem lõpliku korpuse laiendite astmetest (L&N 1.84),
5. Teoreem lõpliku laiendi algebralisusest (L&N 1.85),
6. Teoreem lihtsa laiendi struktuurist (L&N 1.86),
7. Teoreem taandumatu polünoomi lihtsa laiendi olemasolust (L&N 1.87),
8. Teoreem taandumatu polünoomi lihtsa laiendi ühesusest (L&N 1.89),
9. Teoreem polünoomi lahutuskorpuse olemasolust ja ühesusest (L&N 1.91),

10. Teoreem lõplike korpuste olemasolust ja ühesusest (L&N 2.5),
11. Lõpliku alamkorpuse kriteerium (L&N 2.6),
12. Teoreem lõpliku korpuse multiplikatiivse rühma tsüklilisusest (L&N 2.8),
13. Teoreem lõpliku korpuse lõpliku laiendi struktuurist (L&N 2.10),
14. Järeldus lõplike korpuste konstrueeritavuse kohta (L&N 2.11),
15. Lemma polünoomi $x^{q^n} - x$ taandumatute jagajate kohta (L&N 2.13),
16. Teoreem taandumatu polünoomi juurtest (L&N 2.14),
17. Teoreem korpuse $\mathbb{F}_{q^n}$ automorfismidest üle $\mathbb{F}_q$ (L&N 2.21),
18. Elemendi jälje omadused (L&N 2.23),
19. Teoreem jälje seosest lineaarteisendustega (L&N 2.24),
20. Teoreem sellest, millal elemendi jälg võrdub nulliga (L&N 2.25),
21. Teoreem jälje transitiivsusest (L&N 2.26),
22. Elemendi normi omadused (L&N 2.28),
23. Teoreem normi transitiivsusest (L&N 2.29),
24. Duaalbaasi olemasolu (arutelu peale L&N 2.30),
25. Artini lemma (L&N 2.33),
26. Teoreem normaalbaasi olemasolust (L&N 2.35),
27. Teoreem ühejuurte rühma struktuurist (L&N 2.42),
28. Ringpolünoomide põhiomadused (L&N 2.45),
29. Teoreem ringpolünoomi teguritest (L&N 2.47 (ii)),
29. Wedderburni teoreem (L&N 2.55),

32. Elliptilise kõvera arvutusvalemi korrektsus, kus valem on järgmine:

    Olgu $E : y^2 = x^3 + Ax + B$ elliptiline kõver ning $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$ kaks punkti sellel kõveral.

    (i) Kui $P = O$, siis $P \oplus Q = Q$; kui $Q = O$, siis $P \oplus Q = P$;

    (ii) kui $x_1 = x_2$ ja $y_1 = -y_2$, siis $P \oplus Q = O$;

    (ii) muudel juhtudel tähistame

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{kui } P \neq Q, \\ \frac{3x_1^2 + A}{2y_1}, & \text{kui } P = Q \end{cases},$$

    ning

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{ja} \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

    Siis $P \oplus Q = (x_3, y_3)$.

33. Anda ülevaade elliptiliste kõverate (üle lõplike korpuste) Diffie-Hellmani võtmevahetusest ja tõestada viimase korrektsus.