MA2201 - OPPGAVESETT 11

18.48*) La $S \subseteq R$ være s.a. $0_R, 1_R \in S$ og for alle $a, b \in S$ holder $a-b \in S$ og $ab \in S$. Vi ser at $(S, \cdot|_{S\times S})$ er lukket, så trenger kun å vise at $(S, +|_{S\times S})$ er en gruppe. Dette her vi vist på en tidligere øving. Assosiativitet, kommutativitet (addisjon) og distributivitet arves. Vi har at $0_R \in S$, så vi lar $a = 0$ som gir

$$0_R - b = -b \in S, \quad \text{og} \quad b + (-b) = 0,$$

så alle inverser (additive) er med i S. Videre, for $a, b \in S$ $\exists -b \in S$ s.a.

$$a - (-b) = a + b \in S,$$

så S er lukket under addisjon. S er en undervring. ~~Dersom (*) holder~~ Dersom S er en undervring av R så holder (*). □

18.55) La R være en boolsk ring, dvs. $\forall x \in R$ er $x^2 = x$. Vi noterer at dette gir

$$2x = 4x - 2x = 4x^2 - 2x = (2x)^2 - 2x = 2x - 2x = 0,$$

$\forall x \in R$, der $2x = x + x$. Videre gir dette

$$2xy = 0 = (x+y) - (x+y) = (x+y)^2 - (x+y) = x^2 - x + y^2 - y$$

$$+ xy + yx = x - x + y - y + xy + yx = xy + yx.$$

Men additiv forkortingsregel gir $xy = yx$, $\forall x, y \in R$. □

Avsnitt 19

8) Vi ønsker å finne karakteristikken til $\mathbb{Z}_3 \times \mathbb{Z}_3$. Da $\mathbb{Z}_3$ har $n=3$ følger det at $(a,b) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ og

$$n(a,b) = 3(a,b) = (3a, 3b) = (0,0).$$

Altså har vi maks 3 som karakteristikk. Men et element som $(1,0) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ gir 3 som mulige karakteristikk. Altså er karakteristikk 3. ✓

23) La R være en divisjonsring, og la $a \in R$ være s.a. $a^2 = a$. Enten er $a = 0$, eller a har en invers, a^{-1}, som gir

$$a = a^{-1}a^2 = a^{-1}a = 1,$$

så de eneste mulighetene er $a \in \{0,1\}$, da $0^2 = 0$. □ ✓

25) La R være en ring med 1, og ingen nulldivisorer. La $a \neq 0,1 \in R$ og se på

$$A_R = \{a0, a1, ar_2, ar_3, \dots, ar_{n-2}\}, \text{ der } |R| = n.$$

Ingen av disse er like: $ar_i = ar_j \Rightarrow a(r_i - r_j) = 0$ $\Rightarrow r_i = r_j$, dersom $ar_i \neq 0$. Da $|A_R| = n$, må en av elementene være 1, da R er lukket under addisjon. Altså $\exists r \in R$ s.a. $ar = 1$. Tilsvarende $\exists r' \in R$ s.a. $r'a = 1$ ved å studere RA. Men dette gir $r' = r'ar = r$, og hver $a \neq 0,1$ har en unik invers a^{-1}. 1 har 1 som invers. Altså er R en divisjonsring. □ ✓

Avsnitt 20

11) Vi vil løse kongruensen $2x \equiv 6 \pmod 4$, som er ekvivalent med $x \equiv 3 \pmod 2$, eller $x \in 1 + \mathbb{Z}_2$. Altså er løsningene $1+\mathbb{Z}_4$ og $3+\mathbb{Z}_4$. de

13) Vi vil løse kongruensen $36x \equiv 15 \pmod{24}$, som er ekvivalent med $12x \equiv 5 \pmod 8$. Men $\gcd(12,8) = 4 \nmid 5$, så vi har ingen løsning. de

14) Vi vil løse kongruensen $45x \equiv 15 \pmod{24}$, som er ekvivalent med $15x \equiv 5 \pmod 8$. Vi har $\gcd(5,8) = 1$, så det finns $a \in \mathbb{Z}_8$ med $a5 = 5a = 1$, som gir $3x \equiv 1 \pmod 8$. Vi observerer at $3^2 \equiv 1 \pmod 8$, så vi får $x \equiv 3 \pmod 8$, som gir løsningene $3+\mathbb{Z}_8$, eller $3+\mathbb{Z}_{24}$, $11+\mathbb{Z}_{24}$ og $19+\mathbb{Z}_{24}$. $a=5$, dvs $5^{-1} \in \mathbb{Z}_8$ er 5. de

15) Vi vil løse kongruensen $39x \equiv 125 \pmod 9$. Vi har primtalls faktoriseringene

$$39 = 3 \cdot 13$$
$$125 = 5^3$$
$$9 = 3^2,$$

og $\gcd(39,9) = 3 \nmid 125$, altså har ikke kongruensen noen løsning. de

Oppgave

(a) La p være et primtall og $t \geq 1$. Vi vil si hvorfor

$$\varphi(p^t) = |\{1 \leq x \leq p^t \mid \gcd(p^t, x) = 1\}|$$

$$= p^t - |\{1 \leq x \leq p^t \mid \gcd(p, x) > 1\}|$$

$$= p^t - \underbrace{|\{p, 2p, 3p, \ldots, p^{t-1} \cdot p\}|}_{p^{t-1} \text{ elementer}}$$

$$= p^t - p^{t-1} = (p-1)p^{t-1}. \qquad \square$$

(b) La m og n være to hele tall s.a. $\gcd(m,n) = 1$.
Vi vil vise at

$$\varphi(mn) = \varphi(m)\varphi(n).$$

$\mathbb{Z}_m^* = \{\text{grupper av enheter i } \mathbb{Z}_m\}$

$|\mathbb{Z}_m^*| = \varphi(m)$

La $\gcd(m,n)=1$, vis at $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

La $f: \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ ved at $f(x) = (x \bmod m, x \bmod n)$ og $g: \mathbb{Z}_m^* \times \mathbb{Z}_n^* \to \mathbb{Z}_{mn}^*$ ved at $g(x,y) = xy \bmod mn$. Vis at f og g er gruppehom. og at $g \circ f = \mathrm{id}_{\mathbb{Z}_{mn}^*}$ Så er f bijektiv.

La

$(\mathbb{Z}_m^*=) M = \{1 \leq x \leq m \mid \gcd(x, m) = 1\}$

$(\mathbb{Z}_n^*=) N = \{1 \leq x \leq n \mid \gcd(x, n) = 1\}$

$(\mathbb{Z}_{mn}^*=) MN = \{1 \leq x \leq mn \mid \gcd(x, mn) = 1\}$.

Hvorfor? Vi ser at hvert element i MN kan skrives som et produkt av et element i M og N, og hvert element i $M \times N$ gir et produktelement i MN. Følgelig er $M \times N \cong MN$. Altså er

$$\varphi(mn) = |MN| = |M \times N| = |M| \cdot |N| = \varphi(m) \cdot \varphi(n).$$

$\square$