

MATEMATIK, Göteborgs Universitet och Chalmers tekniska högskola
Tentamen i Algebraiska Strukturer (MMG 500, MVE 150 290) 2014-06-11
Inga hjälpmmedel tillåtna
Telefonvakt: 0703-088304 (Anders Martinsson)

1. På mängden $\mathbf{R}_{\geq 0}$ av icke-negativa reella talen införs den binära operationen * genom $m*n = |m - n|$.

- (a) Är operationen * kommutativ på mängden $\mathbf{R}_{\geq 0}$?
- (b) Är operationen * associativ på mängden $\mathbf{R}_{\geq 0}$?
- (c) Finns något neutralt element?
- (d) Om det finns något neutralt element, vilka element har invers?

4p

2. Visa att grupperna S_5 och $S_4 \times \mathbf{Z}_5$ ej är isomorfa.

4p

3. Låt I och J vara ideal i en ring R och $I + J = \{i+j : i \in I, j \in J\}$.

- a) Visa att $I + J$ och $I \cap J$ är ideal i R .
(Glöm inte visa att $I + J$ och $I \cap J$ är additiva grupper.)

4p

- b) I fallet då $R = \mathbf{Z}$ och $I = (m)$ och $J = (n)$ för heltalet så är $I \cap J$ och $I + J$ huvudideal. Ange generatorer för $I + J$ och $I \cap J$.
(Du behöver inte visa att dessa är generatorer.)

1p

4. Visa eller motbevisa att det finns en kropp med n element för

- a) $n=4$
- b) $n=5$
- c) $n=6$.

2p

1p

1p

5. Formulera och bevisa Lagranges sats för delgrupper.

4p

6. Visa att polynom av grad $n \geq 0$ över en kropp har högst n nollställen.
Gäller detta också för polynom över en godtycklig ring?

3p

1p

Alla påståenden måste motiveras utom i 3b)

Solutions to examination in algebra (MMG 500 and MVE 150) 2014-06-11

1a) * is commutative as $x-y$ and $y-x$ have the same absolute value.

1b) * is not associative as $|1-|2-4||=1 \neq ||1-2|-4|=3$.

1c) $|x-0|=|0-x|=x$ for all $x \geq 0$. Hence 0 is neutral.

1d) Each $x \geq 0$ is its own inverse as $|x-x|=0$.

2. There are $4!$ five-cycles $(1, n_1, n_2, n_3, n_4)$ with $n_1, n_2, n_3, n_4 \in \{2, 3, 4, 5\}$ and hence 24 elements of order five in S_5 . But there are only 4 elements of order five in $S_4 \times \mathbf{Z}_5$. To see this, note that $\sigma^5 = id \in S_4$ if $(\sigma, [a]_5)$ is of order five in $S_4 \times \mathbf{Z}_5$. But $o(\sigma) \neq 5$ as $o(\sigma) = |\langle \sigma \rangle|$ is a factor of $|S_4| = 24$ by Lagrange's theorem. Hence $\sigma = id$ and any element of order five in $S_4 \times \mathbf{Z}_5$ of the form $(id, [a]_5)$ with $a \in [a]_5 \in \mathbf{Z}_5^\#$. As there are 24 elements of order five in S_5 and 4 elements of order five in $S_4 \times \mathbf{Z}_5$, these two groups cannot be isomorphic.

3a) We first show that $I \cap J$ is an additive subgroup of R . It is non-empty as $0 \in I \cap J$. It is closed under addition as $a, b \in I \cap J \Rightarrow (a+b \in I \text{ and } a+b \in J) \Rightarrow a+b \in I \cap J$. It is closed under additive inversion as $a \in I \cap J \Rightarrow (-a \in I \text{ and } -a \in J) \Rightarrow -a \in I \cap J$. Hence $I \cap J$ is an additive subgroup by the subgroup criterion. To see that $I \cap J$ is an ideal, let $r \in R$ and $a \in I \cap J$. Then as I and J are ideals, we get that $ra \in I$, $ra \in J$, $ar \in I$ and $ar \in J$. Hence $ra \in I \cap J$ and $ar \in I \cap J$, which proves that $I \cap J$ is an ideal.

To see that $I+J$ is an additive subgroup of R , we first note that $0=0+0 \in I+J$. Further, $I+J$ is additively closed as $(i+j)+(i'+j')=(i+i')+(j+j') \in I+J$ for $i+j, i'+j' \in I+J$. Finally, if $i+j \in I+J$, then $-(i+j)=(-i)+(-j) \in I+J$. Hence $I+J$ is an additive subgroup by the subgroup criterion. Finally, let $r \in R$ and $i+j \in I+J$. Then, $r(i+j)=ri+rj \in I+J$ and $(i+j)r=ir+jr \in I+J$. Hence $I+J$ is an ideal.

3b) If $R=\mathbf{Z}$, $I=(m)$ and $J=(n)$, then $I+J$ is generated by $\gcd(m,n)$ and $I \cap J$ by $\text{lcm}(m,n)$.

4a) $x^2+x+1 \in \mathbf{Z}_2[x]$ is irreducible as it has no zeroes in \mathbf{Z}_2 . Hence $\mathbf{Z}_2[x]/(x^2+x+1)$ is a field by a theorem in Durbin's book. Moreover, from the division algorithm for $\mathbf{Z}_2[x]$, we see that this field has four elements represented by the classes of the four polynomials $ax+b \in \mathbf{Z}_2[x]$.

4b) \mathbf{Z}_5 is a field with five elements as 5 is a prime.

4c) Suppose that L were a field with six elements. Then $1+1+1+1+1=0$ in L as $o(1)=|\langle 1 \rangle|$ is a factor of $|L|$ by Lagrange's theorem for the additive group $(L, +)$. Hence $(1+1)(1+1+1)=0$ by the distributive law. As there are no zero divisors in a field we get that $1+1=0$ or $1+1+1=0$ and that L contains a subfield K isomorphic to \mathbf{Z}_2 or \mathbf{Z}_3 . L is therefore then a vector space over \mathbf{Z}_2 or \mathbf{Z}_3 and of cardinality 2^m or 3^m for some positive integer m . There is thus no field with six elements.

5) See Durbin's book.

6) See Durbin's book.