

TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculteit Wiskunde en Informatica
Tentamen Algebra en Discrete Wiskunde, 2WF50,
Woensdag 15 april 2015, 09:00 – 12:00

Name :

Student number :

Exercise	1	2	3	4	5	6	total
points							

Notes: This exam consists of 6 exercises. You can reach 100 points. The mark for the exam is computed by dividing the total number of points by 10.

Make sure to justify your answers in detail. It is not sufficient to state the correct result without the explanation.

All exercises are stated in Dutch and in English.

Attentie: Dit tentamen bestaat uit 6 opgaven. U kunt maximaal 100 punten behalen. Het cijfer voor het tentamen wordt bepaald door het aantal behaalde punten door 10 te delen.

De uitwerkingen van de opgaven dienen duidelijk geformuleerd en overzichtelijk opgeschreven te worden. Motiveer uw antwoorden, tenzij anders vermeld.

Alle opgaven worden in het nederlands en in het engels gepresenteerd.

1. Let $(\mathbb{C}, +, \cdot)$ denote the field of complex numbers with regular addition and multiplication. Let the sets M_1 and M_2 be defined as follows:

Laat $(\mathbb{C}, +, \cdot)$ het lichaam van de complexe getallen met de gebruikelijke optelling en vermenigvuldiging zijn. Laat de verzamelingen M_1 en M_2 als volgt gedefinieerd zijn:

$$M_1 = \{a + bi\sqrt{1/6} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}, \quad M_2 = \{a + b\sqrt[3]{1/5} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

- (a) State the definition of a ring.
Geef de definitie van een ring. 8 P
- (b) Study whether (M_1, \cdot) is a semigroup.
Ga na of (M_1, \cdot) een halfgroep is. 4 P
- (c) Study whether (M_2, \cdot) is a semigroup.
Ga na of (M_2, \cdot) een halfgroep is. 4 P
- (d) Is $(M_1, +, \cdot)$ a subring of $(\mathbb{C}, +, \cdot)$? Why?
Is $(M_1, +, \cdot)$ een deelring van $(\mathbb{C}, +, \cdot)$? Waarom? 8 P
- (e) Is $(M_2, +, \cdot)$ a subring of $(\mathbb{C}, +, \cdot)$? Why?
Is $(M_2, +, \cdot)$ een deelring van $(\mathbb{C}, +, \cdot)$? Waarom? 2 P

2. Let (M, \cdot) be the group of invertible 2×2 matrices over $\mathbb{Z}/25\mathbb{Z}$, where \cdot is the usual matrix multiplication. We use $\{0, 1, 2, 3, \dots, 24\}$ as representatives of the residue classes modulo 25. Let $N = \{m \in M \mid ad - bc \equiv 1 \pmod{5}\}$.

Laat (M, \cdot) de groep van inverteerbare 2×2 matrices met coëfficiënten in $\mathbb{Z}/25\mathbb{Z}$ zijn met \cdot de matrixvermenigvuldiging. Wij gebruiken $\{0, 1, 2, 3, \dots, 24\}$ als representanten van de restklassen modulo 25. Laat $N = \{m \in M \mid ad - bc \equiv 1 \pmod{5}\}$ zijn.

$$M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}/25\mathbb{Z}, ad - bc \in (\mathbb{Z}/25\mathbb{Z})^\times \right\}.$$

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

- (a) Show that (N, \cdot) is a subgroup of (M, \cdot) .
Toon aan dat (N, \cdot) een ondergroep van (M, \cdot) is. 6 P
- (b) State all left cosets of N in M .
Bepaal alle linkernevenklassen van N in M . 6 P
- (c) Is $\{m \in M \mid ad - bc \equiv 2 \pmod{5}\}$ a subgroup of M ?
Is $\{m \in M \mid ad - bc \equiv 2 \pmod{5}\}$ een ondergroep van M . 3 P

3. Consider the ring $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.
Beschouw de ring $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

- (a) How many elements does R have?
Hoeveel elementen heeft R ? 1 P

- (b) Compute the order of R^\times .
Bereken de orde van R^\times . 3 P
- (c) Compute the (multiplicative) order of $(1, 2, 3) \in R^\times$.
Bereken de (multiplicatieve) orde van $(1, 2, 3) \in R^\times$. 4 P
- (d) Does there exist an integer m such that $R \cong \mathbb{Z}/m\mathbb{Z}$? If so, compute m , give explicit descriptions of the ring homomorphism and the inverse of the ring homomorphism, and compute the image of $(1, 4, 8)$. If not, why not?
Bestaat er een natuurlijk getal m met $R \cong \mathbb{Z}/m\mathbb{Z}$? Zo ja, bereken m , geef expliciete beschrijvingen van het ringhomomorfisme en de inverse van het ringhomomorfisme en bereken het beeld van $(1, 4, 8)$. Zo nee, waarom niet? 14 P
- (e) Find two elements $a, b \in R$ so that $a \cdot b = (0, 0, 0)$ but $a, b \neq (0, 0, 0)$.
Bepaal twee elementen $a, b \in R$ zodat $a \cdot b = (0, 0, 0)$ maar $a, b \neq (0, 0, 0)$. 3 P
- (f) Compute the number of elements $a \in R$ with $a \neq (0, 0, 0)$ for which there exists a $b \neq (0, 0, 0)$ such that $a \cdot b = (0, 0, 0)$. How many such elements exist in R^\times ?
Bereken het aantal elementen $a \in R$ met $a \neq (0, 0, 0)$ waarvoor er een $b \neq (0, 0, 0)$ bestaat met $a \cdot b = (0, 0, 0)$. Hoeveel van zulke elementen bestaan er in R^\times ? 8 P

4. Let G be a group. State the definitions of center $Z(G)$, centralizer $C(X, G)$ and normalizer $N(X, G)$ of a subset $X \subset G$ in G .
Laat G een groep zijn. Geef de definities van centrum $Z(G)$, centralisator $C(X, G)$, normalisator $N(X, G)$ van een verzameling $X \subset G$ in G . 6 P

5. Prove or give a counterexample:
Bewijs of geef een tegenvoorbeeld:

- (a) A prime ideal that is not equal to the whole ring is a maximal ideal.
Een priem ideaal ongelijk aan de hele ring is een maximaal ideaal. 4 P
- (b) A maximal ideal is a prime ideal.
Een maximaal ideaal is een priem ideaal. 4 P

6. (a) State the definition of an algebraic number.
Geef de definitie van een algebraïsch getal. 2 P
- (b) Let $0 < n \in \mathbb{Z}$. Show that $a = e^{2\pi i/n}$ is algebraic and state a polynomial $f_n(x) \in \mathbb{Q}[x]$ with $f_n(a) = 0$. Hint: $e^{\alpha i} = \cos \alpha + i \sin \alpha$ for $\alpha \in \mathbb{R}$.
Laat $0 < n \in \mathbb{Z}$. Toon aan dat $e^{2\pi i/n}$ algebraïsch is en geef een polynoom $f_n(x) \in \mathbb{Q}[x]$ met $f_n(a) = 0$. Hint: $e^{\alpha i} = \cos \alpha + i \sin \alpha$ voor $\alpha \in \mathbb{R}$. 4 P
- (c) Show that $g(x) = x^2 + 1$ factors over \mathbb{F}_p with $p \equiv 1 \pmod{4}$.
Hint: Remember that \mathbb{F}_p^* is cyclic.
Bewijs: $g(x) = x^2 + 1$ factors over \mathbb{F}_p met $p \equiv 1 \pmod{4}$.
Hint: Gebruik dat \mathbb{F}_p^* cyclisch is. 6 P