university of groningen

Algebraic Structures Final Exam

19 June 2020,

15:00 – 18:00 (UTC+02:00)

Instructions – read carefully

- **You have 180 minutes to finish the exam. Immediately after the end of your exam, scan or photograph your answers and email them to `steffen.muller@rug.nl`. You have 15 minutes to do this. Any format is fine, any number of files is fine.**
- **Only after this should you proceed by uploading your solutions to `Exam - Algebraic Structures 19-06-2020`. Upload one `pdf` file which contains your solutions; the name of the file should be your student number, e.g. `s1234567.pdf`. This process should be completed within 45 minutes after the official end time of the exam, so before 18:45.**
- **Start every exercise on a new sheet**
- **The exam consists of 3 questions, each subdivided into 5 parts. You can score up to 36 points and you obtain 4 points for free. Thus you can score between 4 and 40 points in total.**
- **You may freely consult your personal notes and the available course documents. You may NOT consult other people or other sources in any way; you must arrive at your answers independently.**
- **You will get no points if you do not explain your answer. Answers like "Yes", "No" or "123456" will not be accepted. You should submit all useful calculations. No partial credit will be given for correct answers without explanations or computational details.**
- **You must refer to statements in the lecture notes by their number.**
- **When working on a problem in this exam, you may use the statements of *earlier* problems even if you have not solved them. E.g. to solve subproblem (d) of a problem, you may use subproblem (b) of that problem even if you were unable to solve it.**
- **You may not use a calculator or any mathematical software.**
- **You are responsible yourself for starting and stopping the exam on time so make sure you know what time it is.**
- **If you are entitled to extra time, add that extra time to the deadlines mentioned above and send / upload your solutions accordingly. You will get a message that the submission is late; ignore it.**

Each question comes in two versions labeled either A or B (so there are 1A, 1B, 2A, 2B, 3A and 3B). You are only supposed to solve one version of each problem. The version that you have to solve depends on the digits in your student number $\mathsf{s n_1 n_2 n_3 n_4 n_5 n_6 n_7}$:

- If n_3 is even solve 1A, otherwise solve 1B;
- If n_5 is even solve 2A, otherwise solve 2B;
- If n_6 is even solve 3A, otherwise solve 3B.

Notation:

$\mathbb{Z}$ **: Ring of integers**

$\mathbb{Q}$ **: Field of rational numbers**

$\mathbb{R}$ **: Field of real numbers**

$\mathbb{C}$ **: Field of complex numbers**

$\mathbb{F}_q$ **: Finite field with q elements**

Problems

1A. Let $f(X) = X^2 + X + 1 \in \mathbb{Z}[X]$. Let $\omega \in \mathbb{C}$ be a root of f. Then

$$\mathbb{Z}[\omega] = \{a + b\omega \ : \ a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$ (you don't have to show this).

(a) [3 points] Show that $\Phi : \mathbb{Z}[\omega] \to \mathbb{F}_7,\ a + b\omega \mapsto \overline{a + 4b}$ is a ring homomorphism whose kernel is the ideal $I = (7, 3 + \omega)$.

(b) [2 points] Is I prime? Is it maximal?

(c) [2 points] Show that I is principal by finding a generator.

(d) [1 point] Show that $\mathbb{Z}[\sqrt{-3}]$ is a subring of $\mathbb{Z}[\omega]$.

(e) [3 points] Show that $\mathbb{Z}[\omega]$ is Euclidean with $g(a + b\omega) = a^2 + ab + b^2$.

1B. Let $f(X) = X^2 + X - 1 \in \mathbb{Z}[X]$. Let $\zeta \in \mathbb{C}$ be a root of f. Then

$$\mathbb{Z}[\zeta] = \{a + b\zeta \ : \ a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$ (you don't have to show this).

(a) [3 points] Show that $\Phi : \mathbb{Z}[\zeta] \to \mathbb{F}_5,\ a + b\zeta \mapsto \overline{a + 2b}$ is a ring homomorphism whose kernel is the ideal $I = (5, 3 + \zeta)$.

(b) [2 points] Is I prime? Is it maximal?

(c) [2 points] Show that I is principal by finding a generator.

(d) [1 point] Show that $\mathbb{Z}[\sqrt{5}]$ is a subring of $\mathbb{Z}[\zeta]$.

(e) [3 points] Show that $\mathbb{Z}[\zeta]$ is Euclidean with $g(a + b\zeta) = a^2 + ab - b^2$.

2A. Let

$$\mathbb{Q}(X) := \left\{ \frac{f}{g} \ : \ f, g \in \mathbb{Q}[X] \text{ and } g \neq 0 \right\}$$

be the field of fractions of the polynomial ring $\mathbb{Q}[X]$, let $h = X^4 + 3 \in \mathbb{Q}[X]$ and let

$$R := \left\{ \frac{f}{g} \ : \ f, g \in \mathbb{Q}[X] \text{ and } h \text{ does not divide } g \right\} \subset \mathbb{Q}(X).$$

(a) [3 points] Show that R is a subring of $\mathbb{Q}(X)$.

(b) [1 point] Compute the unit group $R^\times$.

(c) [3 points] Show that every $a \in \mathbb{Q}(X) \setminus \{0\}$ can be written in a unique way as $u \cdot h^n$ for some $u \in R^\times$ and $n \in \mathbb{Z}$. (Hint: First consider $a \in \mathbb{Q}[X] \setminus \{0\}$)

(d) [3 points] Compute u and n as in (c) for

$$a = \frac{X^9 - X^8 + 6X^5 - 6X^4 + 9X - 9}{-2X^{10} + 20X^7 - 8X^5 + 12X^3 - 4}$$

(e) [2 points] Show that R has a unique maximal ideal.

2B. Let

$$\mathbb{Q}(X) := \left\{ \frac{f}{g} \ : \ f, g \in \mathbb{Q}[X] \text{ and } g \neq 0 \right\}$$

be the field of fractions of the polynomial ring $\mathbb{Q}[X]$, let $h = X^4 + 2 \in \mathbb{Q}[X]$ and let

$$R := \left\{ \frac{f}{g} \ : \ f, g \in \mathbb{Q}[X] \text{ and } h \text{ does not divide } g \right\} \subset \mathbb{Q}(X).$$

(a) [3 points] Show that R is a subring of $\mathbb{Q}(X)$.

(b) [1 point] Compute the unit group $R^\times$.

(c) [3 points] Show that every $a \in \mathbb{Q}(X) \smallsetminus \{0\}$ can be written in a unique way as $u \cdot h^n$ for some $u \in R^\times$ and $n \in \mathbb{Z}$. (Hint: First consider $a \in \mathbb{Q}[X] \smallsetminus \{0\}$)

(d) [3 points] Compute u and n as in (c) for

$$a = \frac{2X^{10} + 12X^8 - 18X^6 - 24X^2 + 6}{X^9 + X^8 + 4X^5 + 4X^4 + 4X + 4}$$

(e) [2 points] Show that R has a unique maximal ideal.

3A. Let p be a prime and let $f = X^3 + X^2 - 1$ and $g = X^2 + X + 1$ be two polynomials in $\mathbb{F}_p[X]$.

(a) [3 points] Prove that f is irreducible in $\mathbb{F}_p[X]$ if and only if it is irreducible in $\mathbb{F}_{p^2}[X]$.

In (b)–(e) we set $p = 2$ so that f, g are polynomials in $\mathbb{F}_2[X]$. Moreover, we denote by Ω_h the splitting field of $h := f \cdot g$ over $\mathbb{F}_2$.

(b) [3 points] Show that the dimension of Ω_h as a vector space over $\mathbb{F}_2$ is 6.

(c) [3 points] Let α be a root of f and let β be a root of g in Ω_h. Compute the order of $\alpha \cdot \beta$ in the multiplicative group $\Omega_h^\times$.

(d) [2 points] *Prove or disprove:* There exists an element γ in the splitting field Ω_h such that the minimal polynomial of γ over $\mathbb{F}_2$ has degree 4.

(e) [2 points] How many monic irreducible polynomials $r(X) \in \mathbb{F}_2[X]$ are there such that $\mathbb{F}_2[X]/(r)$ is isomorphic to the splitting field Ω_h?

3B. Let p be a prime and let $f = X^3 - X^2 + 1$ and $g = X^2 + X - 1$ be two polynomials in $\mathbb{F}_p[X]$.

(a) [3 points] Prove that g is irreducible in $\mathbb{F}_p[X]$ if and only if it is irreducible in $\mathbb{F}_{p^3}[X]$.

In (b)–(e) we set $p = 3$ so that f, g are polynomials in $\mathbb{F}_3[X]$. Moreover, we denote by Ω_h the splitting field of $h := f \cdot g$ over $\mathbb{F}_3$.

(b) [3 points] Show that the dimension of Ω_h as a vector space over $\mathbb{F}_3$ is 6.

(c) [3 points] Let α be a root of f and let β be a root of g in Ω_h. Compute the order of $\alpha \cdot \beta$ in the multiplicative group $\Omega_h^\times$.

(d) [2 points] *Prove or disprove:* There exists an element γ in the splitting field Ω_h such that the minimal polynomial of γ over $\mathbb{F}_3$ has degree 5.

(e) [2 points] How many monic irreducible polynomials $r(X) \in \mathbb{F}_3[X]$ are there such that $\mathbb{F}_3[X]/(r)$ is isomorphic to the splitting field Ω_h?

GOOD LUCK! ☺