List of exam questions for algebra test (NMAI062)

1. Theory

1.1. Prime factorization and the greatest common divisor.

1. Formulate and prove Fundamental theorem of arithmetic.

2. What are Bezout coefficients (in $\mathbb{Z}$)? Write Euclid's algorithm for the greatest common divisor of natural numbers and explain how to calculate the Bezout coefficients.

1.2. Modular arithmetic.

3. What is a congruence modulo a natural number? Define the Euler's (totient) function φ. Formulate and proof Euler's theorem (about powers to $\varphi(n)$).

4. Formulate and proof The Chinese remainder theorem for integers.

5. Describe how to calculate the value of the Euler's totient function $\varphi(n)$ if we know the prime factorization of n. Prove your claim.

1.3. Fields, rings and domains.

6. What is an integral domain? Write at least two examples of domains which are not fields.

7. For which $n \in \mathbb{N}$ is the ring $(\mathbb{Z}_n, +, -, \cdot, 0)$ a domain? Explain your answer (you can use the claims from the lecture without proof).

1.4. Polynomial rings and quotient fields.

8. Describe the carrier set and operations of the quotient field of a domain. What is the quotient field of integers? And what is the quotient field of a field?

9. Describe the carrier set and operations of a polynomial ring $\mathcal{R}[x]$ over a ring $\mathcal{R}$.

10. Prove that polynomial ring $\mathcal{R}[x]$ over a domain $\mathcal{R}$ is a domain. Does exist a field $\mathcal{F}$ such that $\mathcal{F}[x]$ is a field? Explain your claim.

11. What is a root of a polynomial? Formulate and prove the assertion about number of roots of a polynomial over a domain.

1.5. Divisibility.

12. Define a prime element and an irreducible element. Is every prime element irreducible? Is every irreducible element prime? Explain your claim.

13. What does it mean that two elements of a domain are associated? Describe this relation on a domain using invertible elements.

14. Define a greatest common divisor of two elements of a domain. What is $\gcd(a, 1)$ and $\gcd(a, 0)$ for an element a of a domain?

1.6. Unique factorization domains.

15. Define decomposition of an element into decomposition of a into irreducible elements. Define a unique factorization domain (UFD). Prove that there exists $\gcd(a, b)$ for each pair of elements a, b of a UFD.

16. Formulate a characterization (a necessary and sufficient condition) of a unique factorization domain using the notion of the gcd and chain of divisors. Prove that your condition is sufficient.

1.7. **Calculating greatest common divisors.**

17. Define an Euclidean norm and an Euclidean domain. Write two examples of Euclidean domains (with their norms) which are not fields.

18. What does it mean a primitive polynomial? Formulate Gauss' lemma and Gauss' theorem. If $\mathcal{R}$ is UFD with quotient field $\mathcal{Q}$, explain how to compute greatest common divisors in $\mathcal{R}[x]$ using gcd in $\mathcal{Q}[x]$ and in $\mathcal{R}$.

19. Write the general Euclid's algoritm for Euclidean domain $\mathcal{R}$ and Euclidean norm ν.

20. Prove that each Euclidean domain is a UFD. Is the converse true? Explain your answer.

21. Formulate and prove the Gauss' theorem (you can use all claims from the lecture except the Gauss' theorem, do not forget formulate them).

1.8. **Computing modulo a polynomial.**

22. Describe the construction of a factor (quotient) ring $\mathcal{F}[\alpha]/m(\alpha)$ modulo polynomial $m(\alpha)$ over a field $\mathcal{F}$. Formulate and prove the characterization of those polynomials $m(\alpha)$ such that the factor is a filed.

23. For a prime number p, a natural number n and an irreducible polynomial $m \in \mathbb{Z}$ of degree n, describe the construction of a finite filed of p^n elements. How can be computed inverse elements in this field?

24. Prove that for an arbitrary polynomial f over a filed there exists a filed extension containing a root of f.

25. Formulate and prove The Chinese remainder theorem for polynomials over a filed.

1.9. **Applications.**

26. Describe a (k, n)-secret sharing protocol based on the Chinese remainder theorem for polynomials.

27. Describe the public key protocol RSA and explain why the decryption works properly.

28. Describe the scheme of the Reed-Solomon encoding $\mathbb{F}^k \to \mathbb{F}^n$. Is the encoding an $\mathbb{F}$-linear map? Prove your answer.

1.10. **Groups and subgroups.**

29. Define the notion of a group and its subgroup. What is the order of a group and of an element? Provide an example of a group of order 99.

30. Define the power and the order of an element of a group. Have all elements of a finite group finite order? Explain your answer.

1.11. **Order of a subgroup.**

31. Define the orders of a group and of an element. How does correspond the order of an element and of the corresponding cyclic subgroup? Prove the assertion.

32. Define, formulate, and prove an equivalent description of a subgroup generated by a set.

33. Formulate and prove the Langrange's theorem (about correspondence of orders of a group and its subgroup). What is a left coset of a subgroup?

1.12. **Group actions.**

34. Define the notions of an action of a group on a set X and of the corresponding transitivity relation on X. What does it mean the stabilizer of an element?

35. Formulate and prove the assertion about orbit size and index of stabilizer for an action of a group on a set.

36. Formulate and prove Burnside's lemma (about the number of cosets of the equivalence $\sim$ given by a group action).

1.13. **Cyclic groups.**

37. Describe possible orders and the number of elements of given order in a finite cyclic groups. Prove your claim.

38. If $G = \langle g \rangle$ is finite cyclic group of order n, decide which elements g^n are generators of G. Prove your claim.

39. Prove that a finite subgroup of a multiplicative group of a field is cyclic.

40. What is a discrete logarithm? Describe Diffie-Hellman key exchange / RSA protocol.

2. Types of application and calculation tasks

Values and structures may be changed in tests.

1. Find $u, v \in \mathbb{Z}$ for which $103u + 77v = 1$.

2. Compute the last digit of 33^{999}.

3. Prove that $4x^3 - 15x^2 + 60x + 180$ is irreducible in $\mathbb{Q}[x]$ (use Eisenstein criterion).

4. Compute $2023^{2022^{2021}} \mod 101$.

5. Compute 33^{-1} in the field $(\mathbb{Z}_{37}, +, \cdot, -, 0)$.

6. Solve the system of congruences

$$x \equiv 1(\mod 3), \quad x \equiv 2(\mod 5), \quad x \equiv 1(\mod 7),$$

7. Determine the order of the multiplicative group $(\mathbb{Z}^*_{7\cdot 2^{11}}, \cdot, ^{-1}, 1)$.

8. Construct a field of 125 elements.

9. Show that $m(\alpha) = \alpha^3 + \alpha + 1$ is irreducible in the domain $\mathbb{Z}_7[\alpha]$. Solve the equation $(\alpha^2 + 3)x + \alpha + 4 = \alpha^2$ in the field $\mathbb{Z}_7[\alpha]/(m(\alpha))$.

10. Prove that $\mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$ is a field and compute α^{-1}.

11. Design a secret sharing protocol for 1000 participants such that at least 501 of them are needed to reveal the secret and where the secret is a sequence of 256 bits.

12. Show that $m(\alpha) = \alpha^3 + \alpha + 1$ is irreducible in the domain $\mathbb{Z}_7[\alpha]$. Solve the equation $(\alpha^2 + 3)x + \alpha + 4 = \alpha^2$ in the field $\mathbb{Z}_7[\alpha]/(m(\alpha))$.

13. If $(G, \cdot, ^{-1}, 1)$ is an abelian group, prove that $\{g^n \mid g \in G\}$ is a subgroup of $(G, \cdot, ^{-1}, 1)$ for each $n \in \mathbb{N}$.

14. Decide whether the ring $(\mathbb{Z}_{51}, +, -, \cdot, 0)$ is a domain.

15. Let $f = x^5 + x^2 + x + 1$ and $g = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Calculate $\gcd(f, g)$ and the corresponding Bezout coefficients.

16. Write all irreducible polynomials in $\mathbb{Z}_2[x]$ of degree at most three.

17. Calculate irreducible factorization of the polynomial $2x^2 - 6$ in a) $\mathbb{Z}[x]$, b) $\mathbb{Q}[x]$, c) $\mathbb{C}[x]$.

18. Calculate $\gcd(3 - i, 5 + i)$ in the domain $\mathbb{Z}[i]$.

19. If $(G, \cdot, ^{-1}, 1)$ is an abelian group, prove for each $n \in \mathbb{N}$ that $\{g^n \mid g \in G\}$ is a carrier set of a subgroup of $(G, \cdot, ^{-1}, 1)$.

20. We have four coloured magnets in the shape of an isosceles triangle, whose arms are 1 cm long and have an angle of 45. Eight magnets are yellow, eight blue, eight red, eight green and eight orange. How many different regular octagons can we make from eight of them? Two octagons are considered the same if they differ only in rotation.

21. How many different necklaces (up to rotations and reflections) can you make from four green and four red balls?

22. Compute the number of subgroups of the group $(\mathbb{Z}_{20}, +, -, 0)$ and describe them. Determine the order of the element 18 in $(\mathbb{Z}_{20}, +, -, 0)$.

23. Calculate the index $[\mathbb{Z}_{32} : \langle 24 \rangle]$ in the group $(\mathbb{Z}_{32}, +, -, 0)$.

24. Let $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ be a group and define a mapping $\pi : G \to S_G$ by the rule $\pi(g)(x) = g \cdot x \cdot g^{-1}$. Prove that π is an action of $\mathcal{G}$ on a set G. For which g is 1 a fixpoint?