Mat-2300: Exam 2015

Date: 22.05.2015

Theory

1. What is an equivalence relation on a set S?
2. What is a binary operation on a set S? Which binary operations are called isomorphic?
3. What is a group? What is a subgroup? Give examples.
4. Generators of a group. Cyclic groups and their structure.
5. Homomorphisms and isomorphisms of groups. Kernel, image.
6. Permutation group, its subgroups and Caley's theorem.
7. Cosets (left and right) of a group by a subgroup and Lagrange's theorem.
8. Normal subgroups and factor-groups. Fundamental homomorphisms theorem.
9. Structure of finitely generated Abelian groups.
10. Simple groups. Center and commutator of a group.
11. What is a ring? Define commutative rings, rings with units.
12. Define division rings, integral domains, fields. What is the characteristic of a field?
13. Multiplicative group of a field. Its structure.
14. Homomorphisms and isomorphisms of rings. Kernel, image.

15. The field of quotient of an integral domain. Definition and construction.

16. Ring of polynomials with coefficients in a field: $F[x]$. Degree. Evaluation homomorphism.

17. Factorization of polynomials from $F[x]$. Irreducible and reducible polynomials.

18. Ideals in rings. Factor-rings. Fundamental homomorphisms theorem.

19. Prime ideals and maximal ideals. Quotients by them. Prime fields.

20. Field extensions. Kronecker's theorem. Algebraic and transcendental elements. Degree of an element.

21. What is a vector space over a field? Define degree of a field extension $[E : F]$. Relation between $\deg(\omega, F)$ and $[F(\omega) : F]$.

22. Finite field extensions, algebraic extensions and simple field extensions.

23. Existence of algebraic closure. Structure of Galois fields $GF(p^n)$. Structure of the algebraic closures $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Z}_p}$.

24. Principal ideal domains, unique factorization domains and relations between them.

Exercises

1. Let G be a group and $a, b \in G$ commute: $ab = ba$. Denote $m = \text{ord}(a), n = \text{ord}(b)$. Assume that these numbers are finite and that $\langle a \rangle \cap \langle b \rangle = \{e\}$. Prove that the order $\text{ord}(ab) = \text{lcm}(m, n)$ is the least common multiple of the orders of a, b.

2. Find all cyclic subgroups of the group D_4.

3. Find parity of the permutation $(13572)(2461) \in S_7$ and decompose it into a product of cycles.

4. Find the maximal order of an element of S_n for $n = 6, 7, 8$.
5. Does S_4 contain a normal subgroup of index 5? Does S_5 contains a normal subgroup of index 4?
6. Is it true that $A_3 \simeq \mathbb{Z}_3$? That $\mathbb{Z}_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, $S_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$? That $A_4 \simeq \mathbb{Z}_2^2 \times \mathbb{Z}_3$ or $\mathbb{Z}_3 \times \mathbb{Z}_4$? That $\mathbb{Z}_{12} \simeq \mathbb{Z}_2^2 \times \mathbb{Z}_3$? (Explain)
7. Find the number of generators for the Abelian group $(\mathbb{Z}_n, +)$ for $n = 7, 8, 9, 10$. What is the formula for general n?
8. Prove that if $G \subset S_n$ is a subgroup of order $\mathrm{ord}(G) > 2$, then $H = G \cap A_n$ is a non-trivial subgroup in S_n.
9. Let $(R, +, \cdot)$ be a field and $\phi : (R, +) \to (R, +)$ an isomorphism of the additive group structure. Define the new multiplication by $a \star b = \phi^{-1}(\phi(a) \cdot \phi(b))$. Show that $(R, +, \star)$ is a field with unity $1_\star = \phi^{-1}(1)$ and ϕ is an isomorphism from it to $(R, +, \cdot)$.
10. Compute the multiplication table for the field $(\mathbb{Z}_5, +, \star)$ obtained from the standard field structure of $\mathbb{Z}_5$ as above via the additive isomorphism $\phi : \mathbb{Z}_5 \to \mathbb{Z}_5$ given by $\phi(1) = 2$.
11. Consider the ring $\mathbb{Z}_n^{\mathbb{Z}_n} = \{f : \mathbb{Z}_n \to \mathbb{Z}_n\}$ of $\mathbb{Z}_n$-valued functions on $\mathbb{Z}_n$ with the pointwise addition/multiplication operations. Show that it is isomorphic to the ring $(\mathbb{Z}_n)^n = \mathbb{Z}_n \times \cdots \times \mathbb{Z}_n$ (n times) via the map $\phi : \mathbb{Z}_n^{\mathbb{Z}_n} \to (\mathbb{Z}_n)^n$:

$$\phi(f) = (f(0), f(1), \ldots, f(n-1)).$$

12. Consider the quadratic polynomial $P_a(x) = x^2 - a$. Find for which a it is irreducible over the fields $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$.
13. Prove that for any prime $p > 2$ there are exactly $\frac{p-1}{2}$ irreducible polynomials among $P_a(x) = x^2 - a$ over $\mathbb{Z}_p$.
14. Let p be prime. Prove that $P(x) = x^p - x$ is completely reducible over $\mathbb{Z}_p$ (decomposes into linear factors).
15. Let $\omega \in \mathbb{C}$. Find $\deg(\omega, \mathbb{R})$ and $\deg(\omega, \mathbb{C})$.
16. Let $\omega = e^{\pi i/n}$ for $n = 2, 3, 4, 5, 6$. Find $\deg(\omega, \mathbb{Q})$.
17. Find $\deg(e, \mathbb{Q})$, $\deg(e^2, \mathbb{Q})$ and $\deg(e^i, \mathbb{Q})$.

18. For the fields $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ check if ω is algebraic over F and find $\mathrm{irr}(\omega, F)$ (if yes) and $\deg(\omega, F)$ for the following numbers: $\omega = \frac{\sqrt{3}}{2} + \frac{i}{2}$; $\omega = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$; $\omega = \cos 1 + i \sin 1$.

19. Let E be the minimal field extension of $\mathbb{Q}$ containing all roots of the equations $x^m = n$ for $n, m \in \mathbb{N}$. Find $\dim_{\mathbb{Q}} E$ and $\dim_E \mathbb{R}$.

20. Let $R = F(x)$ be the field of rational functions with coefficients in F. Show that it is a field extension of F and find $\deg(x, F)$.

21. Let $P \in F[x]$ be an irreducible polynomial and $E = F[x]/P$ the field extension. What is $\deg(x, F)$ here?

22. Describe explicitly the field $GF(n)$ for $1 \leq n \leq 10$.

23. Find whether the following is true or false:
    - $\mathbb{Z}_2 \subset GF(3)$? • $\mathbb{Z}_2 \subset GF(2^3)$? • $GF(2^3) \subset GF(2^4)$?
    - $GF(2^2) \subset GF(2^4)$? • $GF(3) \subset GF(2^4)$? • $GF(2^3) \subset \overline{\mathbb{Z}_2}$?

24. Find all units for the rings $\mathbb{Z}, \mathbb{Z}_5, \mathbb{Z}_{12}, \mathbb{Q}$ and also $\mathbb{Z}[x], \mathbb{R}[x]$.

25. Is $\mathbb{Z}[x, y]$ a PID? Is it a UFD? Is it Noetherian?