MB104 – okruhy ke zkoušce

1. Algebra
    - struktury s jednou operací, jejich podstruktury a homomorfismy
    - podrobněji – grupy permutací, grupy zbytkových tříd, dihedrální grupy,
    - homomorfismy a související pojmy, (přímý) součin grup
    - řád prvku, cyklická grupa, čínská zbytková věta
    - rozklady (faktorizace) grup – Lagrangeova věta a její důsledky, normální podgrupy, vztah mezi normálními podgrupami a homomorfismy, určování struktury faktorgrupy
    - okruh, obor integrity, těleso
    - okruhy polynomů, polynomiální funkce - kořeny
    - dělitelnost polynomů, ireducibilita (obecně i nad konkrétními číselnými obory, Eisensteinovo kritérium ireducibility), kořenový činitel, násobnost kořenů, základní věta algebry
    - kryptografie – RSA, Diffie-Hellman
    - uspořádané množiny – základní pojmy, hasseovský diagram, svaz a základní vlastnosti, kritérium distributivnosti svazu
    - Booleovské algebry – definice, vlastnosti, výroková logika, normální tvar výrokových formulí, homomorfismus Booolevských algeber
2. Pravděpodobnost a statistika
    - základní prostor, jevové pole, pravděpodobnost a její základní vlastnosti
    - klasická pravděpodobnost
    - geometrická pravděpodobnost
    - podmíněná pravděpodobnost, Bayesova věta
    - náhodná veličina – definice, diskrétní/spojitá, distribuční funkce a její vlastnosti, pravděpodobnostní funkce, hustota
    - základní typy rozdělení diskrétních a spojitých náhodných veličin
    - transformace náhodných veličin
    - normální rozdělení a rozdělení od něj odvozená
    - číselné charakteristiky náhodných veličin – základní vlastnosti střední hodnoty a rozptylu, momentová vytvořující funkce, kvantily
    - limitní věty – Moivre-Laplace, Čebyševova nerovnost, zákon velkých čísel, Bernoulliova věta, centrální limitní věta
    - náhodný vektor, simultánní a marginální distribuční funkce
    - charakteristiky náhodných vektorů
    - náhodný výběr – definice, základní statistiky
    - náhodný výběr z normálního rozdělení
    - dvouvýběrové statistiky
    - bodové odhady parametrů – nestrannost, asymptotická nestrannost, porovnání odhadů
    - interval spolehlivosti – definice, případ normálního rozdělení
    - testování hypotéz – interval spolehlivosti, kritický obor, p-hodnota; oboustranná vs. jednostranná alternativa
    - testy hypotéz o parametrech normálního rozdělení