The lists of definitions and statements
Algebra,
Dima Trushin

CS NRU HSE, 2023/2024, DSBA

Definitions

1. A binary operation. Definition 4.
2. Associative operation. Defintion 7.
3. A neutral element. Definition 9.
4. An inverse element in case of a binary operation. Definition 12.
5. A group. Definition 17.
6. An abelian group. Definition 17.
7. The group $\mathbb{Z}_n$. Example 18 item 4.
8. The group $\mathbb{Z}_n^*$. Example 18 item 5.
9. A subgroup. Definition 19.
10. A cyclic subgroup. Definition 22.
11. The order of an element of a group. Definition 24.
12. A coset in a group. Definition 29.
13. A normal subgroup. Definition 32.
14. The index of a subgroup. Definition 38.
15. A homomorphism of groups. Definition 40.
16. An isomorphism of groups. Definition 44.
17. The kernel of a homomorphism of groups. Definition 46 item 1.
18. The image of a homomorphism of groups. Definition 46 item 2.
19. A product of groups. Definition 48.
20. A ring. Definition 60.
21. A field. Definition 60.
22. The ring $\mathbb{Z}_n$. Example 61 item 5.
23. A subring. Definition 63.
24. An invertible element of a ring. Definition 65.
25. A zero divisor of a ring. Definition 65.
26. A nilpotent element of a ring. Definition 65.
27. An idempotent element of a ring. Definition 65.
28. An ideal. Definition 67.
29. A homomorphism of rings. Definition 70.
30. An isomorphism of rings. Definition 70.
31. The kernel of a ring homomorphism. Definition 74.
32. The image of a ring homomorphism. Definition 74.
33. A greatest common divisor of two polynomials. Definition 81.
34. An irreducible polynomial in one variable. Definition 86.
35. The ring of polynomial remainders. The beginning of Section 6.4 before Claim 89.
36. The characteristic of a field. Definition 93.
37. An extension by a root for fields. Section 7.2.
38. A lexicographical order on monomials. Definition 108.
39. The leading term of a polynomial. Definition 113.
40. An elementary reduction of a polynomial with respect to another one. Definition 114.
41. A reduction of a polynomial with respect to a set of nonzero polynomials. Definition 116.
42. A remainder of a polynomial with respect to a set of nonzero polynomials. Definition 116.
43. A Gröbner basis. Definition 118.
44. The S-polynomial of two polynomials. Definition 123.
45. A finitely generated ideal. Definition 129.

Statements

1. Classification of of cyclic groups. Claim 26.
2. Structure of subgroups of $\mathbb{Z}$. Claim 27.
3. Structure of subgroups of $\mathbb{Z}_n$. Claim 28.
4. Equivalent definitions of a normal subgroup. Claim 33.
5. Formulas for the number of cosets in a finite group. Claim 37.
6. The Lagrange Theorem. Claim 39.
7. The relation between the order of an element the order of a group. Corollary 2 of Claim 39.
8. A group of a prime order. Corollary 4 of Claim 39.
9. The Fermat Little Theorem. Corollary 5 of Claim 39.
10. Properties of the kernel of a group homomorphism. Claim 47 items 2 and 4.
11. Properties of the image of a group homomorphism. Claim 47 items 1 and 3.
12. The Additive Chinese Remainder Theorem for integers. Claim 52.
13. Classification of finite abelian groups. Claim 54.
14. The Multiplicative Chinese Remainder Theorem for integers. Claim 56.
15. Cryptography. Describe Diffie-Hellman communication process. Section 4.4.
16. Ideals of the ring $\mathbb{Z}$. Claim 68.
17. Ideals of the ring $\mathbb{Z}_n$. Claim 69.
18. Properties of the kernel of a ring homomorphism. Claim 75 items 2 and 4.
19. Properties of the image of a ring homomorphism. Claim 75 items 1 and 3.
20. Ideals of the polynomial ring in one variable. Claim 82.
21. The relation between gcd of two polynomials and the polynomials. Claim 83 item 1.
22. UFD property of the polynomial ring in one variable. Claim 87.
23. Ideals of a ring of polynomial remainders. Claim 91.
24. The Chinese Remainder Theorem for the ring of polynomial remainders. Claim 92.
25. Options for the characteristic of a field. Claim 95.
26. When a ring of integer remainders is a field. Claim 98.
27. Number of elements of a finite field. Claim 103.
28. Structure of the multiplicative group of a finite field. Claim 104.
29. Classification of finite fields. Claim 105.
30. Describe the Galois random generator. Section 7.4.
31. The property of a descending chain of monomials. Claim 111.
32. Membership problem and how to solve it. Section 8.7.
33. Variable elimination problem and how to solve it. Section 8.7.
34. The Buchberger Criterion. Claim 125.
35. S-polynomial in case of coprime leading monomials. Claim 127.
36. The Diamond Lemma. Claim 132.