Problems of Chapter 2

Wednesday, September 16, 2020 8:35 PM

1. A semigroup is a set S with binary operation o:SxS-->S which is associative, ao(boc)=(aob)oc. First observe that a^n=aoa^(n-1) by induction and is also a^(n-1)oa by associativity.
   To prove (2.2):
   a^noa^m=(a^(n-1)oa)oa^m=a^(n-1)o(aoa^m)= a^(n-1)o(a^(m+1)). Then prove by induction that a^noa^m=a^(n+m).
   To prove (2.3):
   (aob)^n=a^nob^n. Follow on similar lines by splitting a^n=aoa^(n-1) then by associativity.

2. An operation on {0,1} is any binary Boolean function. Binary means of two variables. We can then have for any one such function
   f(0,0)=a, f(0,1)=b, f(1,0)=c, f(1,1)=d where a,b,c,d are 0 or 1. There are 2^4=16 such functions. Now check which of these satisfy associativity. Then that function gives a semigroup. For example the function
   F(0,0)=1, f(0,1)=1, f(1,0)=0, f(1,1)=0 is not associative, ((0,0),1)=(1,1)=0 while (0,(0,1))=(0,1)=1

3. If e1 and e2 are two neutral elements then by definition e1oe2=e1=e2.

4. After finding out all functions which form semigroups of {0,1}, check for existence of identity element to discover monoides. For a group all elements must have inverses.

5. If aob=e and aoc=e then a^{-1}o(aob)=a^{-1}o(aoc) gives b=c.

6. The map given as Z/m-->Z/n takes a mod m to a mod n. But as n<m, a mod m=a mod n. The map respects sums (a+b) mod m = (a mod m+b mod m) mod m and ab mod m=(a mod m)(b mod m) mod m hence the map is a homomorphism. For any element a in Z/n there is at least one preimage a itself in Z/m. Hence it is surjective.

7. Consider Z/4={0,1,2,3}. Then 2.3=2=2.1 but 3 is not equal to 1. Hence cancellation does not hold. (in general in Z/m there are zero divisors which are not invertible hence cannot be cancelled).

8. Z/16={0,1,2,…,15}. Invertible elements are (coprime to 2), hence all odd numbers {1,3,5,..,15} this is the group of units (Z/16)^*. Zero divisors are {2,4,6,8,..,14}.

9. If R is a ring and R^* the set of invertible elements with product o as binary operation, then o is associative, there is the unit element 1 and every element is invertible. Hence (R^*,o) is a group.

10. 122x=1 mod 343. Find d=gcd(343,122)=1. Then by extended Euclid find a,b such that 122x+343y=1. If gcd is not 1 then there is no solution.

11. ax=b mod m iff ax+qm=b hence soln exists iff gcd (a,m)|b. Let the gcd be d. Then for a=da1, m=dm1, a1,m1 are coprime. Hence by ext Euclid you have a1x+m1y=1 find all such x,y. Then ax=d mod m.

12. High school problem.

13. Invertible elements of Z/25 are elements coprime to 5. Hence {1,2,3,4,6,7,8,9,11,...24} find their inverses mod 25. For example 2.13=1 mod 25, 3.17=51=1 mod 25.

14. Easy exercise. Show that lcm(a,b)gcd(a,b)=ab.

15. Set theory pigeon whole principle. Or simply replace each element of X by the image in Y. Then you have |X|\leq|Y| and |Y|\leq |X| hence they are equal. Is this true for infinte sets?

16. Subgroup generated by powers of 2 in Z/17. {1,2,4,8,16}.

17. Prime factors of 1234=2*617. 617 is prime. Hence order 2 must be either 617 or 1234.

18. Compute orders.

19. 2^20 mod 7=2^(20 mod 6)mod 7 by Fermat's little theorem. Hence 2^20 mod 7=2^2 mod 7=4.

20. Proved in class notes.

21. Given p=3 mod 4 and there is x such that a=x^2 mod p. Then (p+1)=0 mod 4 hence b=a^{(p+1)/4} mod p is defined. If p|a then the result is trivial. So assume p does not divide a. Then b^4=a^(p+1) mod p=a^2 mod p by Fermat's theorem. Hence we have (b^2+a)(b^2-a)=0 mod p which shows that b^2=\pm a mod p I.e. b is a square root of a mod p.

22. Proof by construction. Done in previous class.
23. First note that 1237 is prime. Then find a primitive root z of Z/1237. Then use the formula ord (z)^k=1236/gcd(k,1236)=103. From this compute k after computing prime factorization of 1236.

24. G is cyclic group of order n and g is a primitive element, then all powers of g generate G. The homomorphism is g^{(x+y) mod n}=g^xg^y. For each x in Z/n there is a unique power of g in G hence this is an isomorphism.

25. X=[(3.5.7)(3.5.7)^{-1} mod 2+(2.5.7)(2.5.7)^{-1} mod 3+ (2.3.7)(2.3.7)^{-1} mod 5+(2.3.5)(2.3.5)^{-1} mod 7] mod 2.3.5.7 =1+1+2.3+2.4=16

26. Divide and check by irreducible polynomials of deg 3,4,5.

27. Search over p. May need lot of computation.

28. Group of finite field F_5 has 4 elements. Hence all irreducible polynomials of degree 5 which generate the field whose groups are all the required groups.