

MATH 113, HOMEWORK 3 SOLUTIONS

ALLEN KNUTSON

All page numbers refer to [F].

p85 #26,32,33,40,52,54,56,62,63.

#26. The whole group $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. The maximal subgroups are $\{0, 2, 4, 6, 8, 10\}$ and $\{0, 3, 6, 9\}$; the others are $\{0, 4, 8\}$, $\{0, 6\}$, and just $\{0\}$. You can figure out the lattice diagram from there.

#32. All the divisors of 20: 1,2,4,5,10,20.

#33. Likewise: 1,17.

#40. "Only if", but not "if". This only guarantees that the order divides n , not necessarily that it's equal to n .

#52. In fact all that matters is that G is generated by a , i.e. every g is of the form a^k for some $k \in \mathbb{Z}$, and ϕ is a group homomorphism.

Then $\phi(g) = \phi(a^k) = \phi(a)^k$ – knowing $\phi(a)$ tells us what $\phi(g)$ must be, for each g .

#54. $(ba)^n = bababa \dots ba = b(ab)^n b^{-1} = b \mathbf{1} b^{-1} = \mathbf{1}$. So ab of order n implies ba has order dividing n . In reverse, ba of order k implies ab has order dividing k , so k and n are positive integers dividing each other and must be equal.

#56. Two cases: either (I) G has an element a of infinite order, or else (II) every element is of finite order.

Case I: Let's prove that if G is infinite, then it has infinitely many subgroups (the contrapositive of the original statement).

Inside $\langle a \rangle$ there are already an infinite number of subgroups, one for each natural number n , namely $\langle a^n \rangle$. Ta-da, an infinite number of subgroups.

Case II: Let's prove that if G has finitely many subgroups, then it's finite (the original statement, directly).

Each element of G is in a cyclic subgroup (in particular, the one it generates). So G is the union of its cyclic subgroups. Each of those is finite, by assumption. So G is a finite union of finite sets, therefore finite.

#62,63. Since G is cyclic, let's pick a generator a . Every element of G is of the form a^k , so we're counting solutions to $(a^k)^m = e$.

Since a is of order n , the only powers of it that are the identity are the multiples of n (division of km by n with remainder, must produce zero remainder). So $km = np$ for some $p \in \mathbb{Z}$.

In question #62: divide this by m to say k is a multiple of the integer n/m . There are exactly m such multiples in $[0, n)$.

Date: October 6, 2000.

In question #63: divide $n \mid km$ by $d := \gcd(m, n)$ to get $n/d \mid k(m/d)$. Now since n/d and m/d have no common factor, this implies $n/d \mid k$. There are exactly d such multiples k in $[0, n)$. So the number of solutions is not m but $\gcd(m, n)$. (Note that $m = \gcd(m, n)$ exactly if $m \mid n$.)

REFERENCES

[F] John B. Fraleigh, A First Course in Abstract Algebra, 6th edition

E-mail address: `allenk@math.berkeley.edu`