Lorenz Halbeisen*

Group Theory (Module 210PMA208)

Department of Pure Mathematics

Week 6, 2002

You may download the ps-file from
http://www.math.berkeley.edu/~halbeis/4students/gt.html

Please hand in your solutions (stapled together with your full name on the first page) at the lecture on Monday, 11 March 2002.

---

26. (a) What is the order of the group $(\mathbb{Z}_{17}^*, \cdot)$?
    (b) Compute the order of 2 in the group $(\mathbb{Z}_{17}^*, \cdot)$.
    (c) Compute the order of 6 in the group $(\mathbb{Z}_{17}^*, \cdot)$.
    (d) Find an element in $\mathbb{Z}_{17}^*$ of order 4.
    (e) Find an element $x \in \mathbb{Z}_{17}^*$ such that $x^3 \equiv_{17} 13$.
    (f) Which of the numbers $2^{888} - 1$, $6^{888} - 1$ and $15^{444} + 1$ is a multiple of 17 ?
27. (a) What is the order of the group $(\mathbb{Z}_{15}, +)$?
    (b) What is the order of 3 in the group $(\mathbb{Z}_{15}, +)$?
    (c) Why is $(\mathbb{Z}_{15}^*, \cdot)$ not a group?
    (d) For which $a \in \mathbb{Z}_{15}^*$ there is a number $b \in \mathbb{Z}_{15}^*$ such that $a \cdot b \equiv_{15} 1$?
28. Let $m \geq 2$. An element $a \in \mathbb{Z}_m^*$ is called *invertible* if there is a number $b \in \mathbb{Z}_m^*$ such that $a \cdot b \equiv_m 1$.
    Show that $a \in \mathbb{Z}_m^*$ is invertible if and only if $\gcd(a, m) = 1$.
29. Let $m \geq 2$ and let $\varphi(m) = \big\{a \in Z_m^* : \gcd(a, m) = 1\big\}$.
    (a) Evaluate $\varphi(15)$.
    (b) Show that $\big(\varphi(m), \cdot\big)$ is a group.
    (c) What is the order of the group $\big(\varphi(12), \cdot\big)$?
30. (a) What is the order of the group $\big(\varphi(18), \cdot\big)$?
    (b) What is the order of 7 in $\big(\varphi(18), \cdot\big)$?
    (c) What is the order of 5 in $\big(\varphi(18), \cdot\big)$?
    (d) Which of the numbers $5^{333} - 1$, $43^{333} - 1$ and $11^{333} + 1$ is a multiple of 18 ?

---

*David Bates Building, Room 1014.
Office hours: Monday 3 pm–4 pm, Friday 1 pm–2 pm