Modern Algebra

Practice Exam - Solutions

Disclaimer: This practice exam is not intended to reflect the content of Wednesday's midterm. It is simply a list of problems left over from the preparation of the actual exam, and should serve to indicate the general format and difficulty level thereof. Solutions will be posted Monday evening.

Problem 1. Let G be a finite group. Show that the number of elements in G of order greater than 2 must be even. Conclude that any group of even order must contain an element of order 2.

Solution. This is really just a simple counting argument. Let S be the set of all elements of G with order greater than two. If $S = \emptyset$ then $|S| = 0$ and we're finished. So assume $S \neq \emptyset$. Since $|x| = |x^{-1}|$ for any $x \in G$, we see that $x \in S$ if and only if $x^{-1} \in S$. Moreover, if $x \in S$ then $x^2 \neq e$ so that $x \neq x^{-1}$. It follows that S can be written as the disjoint union of two element sets of the form $\{x, x^{-1}\}$, and hence that $|S|$ is even.

Suppose that $|G|$ is even. Since e has order 1, $e \notin S$. It follows that $G \setminus S \neq \emptyset$. So $0 < |G \setminus S| = |G| - |S|$. Since $|G|$ and $|S|$ are both even, it follows that $|G \setminus S|$ is a nonzero even integer, i.e. is at least 2. Thus, there is an $x \in G \setminus S$, $x \neq e$. Since S consists of all elements in G of order greater than 2, it must be the case that $|x| = 2$.

Problem 2. A group G is called *divisible* if given any $x \in G$ and any $n \in \mathbb{Z}^+$ there exists a $y \in G$ so that $y^n = x$.

(a) Show that $\mathbb{Q}$ (with the operation of addition) is divisible.

(b) Show that a cyclic group is never divisible.

Solution. (a) Let $x \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$. Then $y = x/n \in \mathbb{Q}$ and

$$ny = n\frac{x}{n} = \underbrace{\frac{x}{n} + \frac{x}{n} + \cdots + \frac{x}{n}}_{n \text{ terms}} = x$$

which expresses the divisibility property in additive form.

(b) Let $G = \langle g \rangle$ be a cyclic group. Suppose first that G is infinite. Take $x = g$ and $n = 2$. For any $y \in G$ there is an $m \in Z$ so that $y = g^m$ so that $y^2 = g^{2m}$. Thus, if $y^2 = g$ then $2m = 1$, which is impossible. Therefore, G is not divisible.

If G is finite, choose any $x \in G$, $x \neq e$, and let n be the LCM of all of the orders of elements in G. Then for any $y \in G$ we have $y^n = e \neq x$, so that G is not divisible. Note that in the finite case we never had to use the fact that G was cyclic!

Problem 3. Let G be a *finite* group and let H be a subgroup of G. The *normalizer of H in G* is

$$N(H) = \{x \in G \,|\, xhx^{-1} \in H \text{ for all } h \in H\}.$$

Show that $N(H)$ is a subgroup of G.

Solution. We use the finite subgroup test. It is clear that $e \in N(H)$ so that $H \neq \emptyset$. Let $x, y \in N(H)$. Then for any $h \in H$ we have $yhy^{-1} = h' \in H$. Thus

$$(xy)h(xy)^{-1} = x(yhy^{-1})x^{-1} = xh'x^{-1} \in H$$

since $x \in N(H)$. It follows that $xy \in H$. Since G is finite, $N(H)$ is finite, and the finite subgroup test implies $N(H) \leq G$.

Problem 4. Show that $U(11)$ is cyclic. Use this fact to compute the remainder when 104^{2006} is divided by 11.

Solution. We see that $2 \in U(11)$ and

$$\begin{aligned}
2^2 \bmod 11 &= 4\\
2^3 \bmod 11 &= 8\\
2^4 \bmod 11 &= 16 \bmod 11 = 5\\
2^5 \bmod 11 &= 2 \cdot 5 \bmod 11 = 10\\
2^6 \bmod 11 &= 2 \cdot 10 \bmod 11 = 9\\
2^7 \bmod 11 &= 2 \cdot 9 \bmod 11 = 7\\
2^8 \bmod 11 &= 2 \cdot 7 \bmod 11 = 3\\
2^9 \bmod 11 &= 2 \cdot 3 \bmod 11 = 6\\
2^{10} \bmod 11 &= 2 \cdot 6 \bmod 11 = 1.
\end{aligned}$$

Hence, $|2| = 10 = |U(11)|$, so that $U(11) = \langle 2 \rangle$.

Since $104 \bmod 11 = 5$, we know that $104^{2006} \bmod 11 = 5^{2006} \bmod 11$. Since $U(11)$ is cyclic of order 10, the order of 5 must divide 10. Since $2006 = 2000 + 6 = 200 \cdot 10 + 6$ it follows that

$$5^{2006} \bmod 11 = (5^{10})^{200} 5^6 \bmod 11 = 1^{200} 5^6 \bmod 11 = 5^6 \bmod 11.$$

Our computations above show that

$$5^6 \bmod 11 = (2^4)^6 \bmod 11 = 2^{24} \bmod 11 = 2^4 \bmod 11 = 5.$$

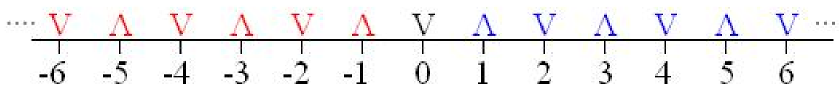
Thus, the remainder when 104^{2006} is divided by 11 is 5.

Problem 5. Determine the elements of the group of symmetries of an infinite string of alternating Λ's and V's:

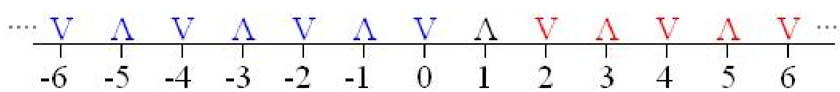
$$\cdots \Lambda\text{V}\Lambda\text{V}\Lambda\text{V}\Lambda\text{V} \cdots$$

Solution. We proceed as we did with the symmetries of the infinite string of $H's$. Let G denote the group of symmetries. In the xy-plane, write the string of Λ's and V's along the x-axis, with the V's above the even integers and the Λ's above the odd integers. Color those letters above the positive integers blue, and those above the negative integers red, leaving the V above 0 black. Let E denote the identity transformation, R the rotation about the point midway between the black V and the first blue Λ, F the flip across the y-axis and T_2n the translation of the black V by $2n$ units. The outcome of each of these transformations is illustrated below.

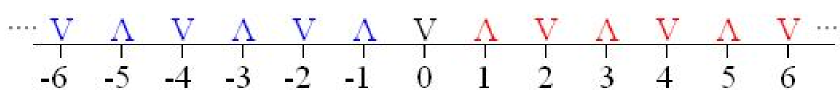
E



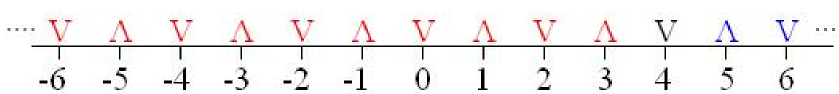
R



F



T_4



Let $S \in G$. Then S carries the V above 0 to some other V or Λ, say at the mth position. Write $m = 2n + \epsilon$, where $\epsilon = 0$ if the central V is mapped to another V and $\epsilon = 1$ if the central V ends up as a Λ. Then $T_{-2n}S$ carries the central V onto either the central V when $\epsilon = 0$ and onto the first blue Λ when $\epsilon = 1$. It follows that $R^{\epsilon}T_{-2n}S$ carries the central V onto itself. There are only two elements of G that do this: E or F. Hence, $R^{\epsilon}T_{-2n}S = F^{\delta}$, where $\delta = 0$ or 1. Since R is its own inverse, and $T_{-2n} = T_{2n}^{-1}$, we see that

$$S = T_{2n}R^{\epsilon}F^{\delta}.$$

It follows immediately that

$$G = \left\{ T_{2n} R^{\epsilon} F^{\delta} \,|\, n \in \mathbb{Z},\ \epsilon, \delta \in \{0, 1\} \right\}.$$