

Solution to Homework # 11 (week of 11/1–11/5)

Due Friday, 11/05/04 in class

1. (**12 points total**) We follow that suggestions given in class. Let $G = S_n$, where $n \geq 3$, and $f : G \rightarrow \overline{G}$ be a group homomorphism, where \overline{G} is *commutative*. Let $\sigma \in G$ be a 3-cycle. Since $|\sigma| = 3$ it follows that $|f(\sigma)|$ divides 3. Now $\sigma = \tau\tau'$, where τ, τ' are 2-cycles of G . Since $|\tau| = |\tau'| = 2$ it follows that $|f(\tau)|, |f(\tau')|$ divide 2. Now

$$f(\sigma)^2 = (f(\tau\tau'))^2 = (f(\tau)f(\tau'))^2 = f(\tau)^2 f(\tau')^2 = e'e' = e'.$$

The third equation follows since $f(\tau)$ and $f(\tau')$ commute. This calculation shows that $|f(\sigma)|$ divides 2. As $|f(\sigma)|$ divides 3 as well, necessarily $|f(\sigma)| = 1$. Thus $f(\sigma) = e'$.

We have shown that $\sigma \in \text{Ker } f$. Since the latter is a subgroup of G , and all even permutations are products of 3-cycles, $A_n \subseteq \text{Ker } f$.

Let $\tau \in G$ be a 2-cycle and let $\sigma' \in G$ be an odd permutation. Then $\sigma' = \tau\sigma$, where $\sigma = \tau^{-1}\sigma'$. Since τ is odd necessarily σ is even. Thus

$$f(\sigma') = f(\tau\sigma) = f(\tau)f(\sigma) = f(\tau)e' = f(\tau).$$

We have shown that $\text{Im } f = \{e', f(\tau)\}$.

Case 1: $f(\tau) = e'$. Then $f : G \rightarrow \overline{G}$ is given by $f(\sigma) = e'$ for all $\sigma \in G$.

Case 2: $f(\tau) \neq e'$. In this case $f(\tau) = b$ has order 2. Thus

$$f(\sigma) = \begin{cases} e' & : \sigma \text{ even;} \\ b & : \sigma \text{ odd.} \end{cases}$$

The reader is left to check that the function f described in Case 2 is indeed a homomorphism. (**7 points for the analysis**)

Now let $m, n \geq 1$ and $\overline{G} = \mathbf{Z}_m$. Then $f : S_n \rightarrow \mathbf{Z}_m$ given by $f(\sigma) = 0$ for all $\sigma \in S_n$ is a homomorphism. (2 points)

Suppose that $f : S_n \rightarrow \mathbf{Z}_m$ is a non-zero homomorphism. Then $n > 1$. Let $\tau \in S_n$ be a 2-cycle. Then $f(\tau)$ has order 2. (If $n = 2$ this is the case since $S_2 = \{\text{Id}, \tau\}$. If $n \geq 3$ this follows by Case 2 above.) Thus m must be even. In this case \mathbf{Z}_m has a unique element of order 2, namely $m/2$. Thus

$$f(\sigma) = \begin{cases} 0 & : \sigma \text{ even;} \\ \frac{m}{2} & : \sigma \text{ odd.} \end{cases} \quad (3 \text{ points})$$

2. (16 points total) a) Since G is finite $|G| = |\text{Ker } f| |\text{Im } f|$. Since f is onto $|\text{Im } f| = |\overline{G}|$. The two preceding equations show that $|\overline{G}|$ divides $|G|$. Since $\overline{G} = f(G) = f(\langle a \rangle) = \langle f(a) \rangle$ it follows that \overline{G} is cyclic and generated by $f(a)$. (4 points)

b) *Well-defined.* Suppose that $a^\ell = a^{\ell'}$, where $\ell, \ell' \in \mathbf{Z}$. Since $|G|$ is the order of a it follows that $|G|$ divides $\ell - \ell'$. Now $|\overline{G}|$ divides $|G|$. Therefore $|b| = |\overline{G}|$ divides $\ell - \ell'$. This means $b^\ell = b^{\ell'}$.

Homomorphism: Any two elements of G have the form a^ℓ and a^m for some $\ell, m \in \mathbf{Z}$. The calculation $f(a^\ell a^m) = f(a^{\ell+m}) = b^{\ell+m} = b^\ell b^m = f(a^\ell) f(a^m)$ shows that f is a homomorphism. (4 points)

c) By parts a) and b) the onto homomorphisms $f : G \rightarrow \overline{G}$ are given by $f(a^\ell) = c^\ell$ for all $\ell \in \mathbf{Z}$, where c generates \overline{G} . The elements c are given by $c = b^r$, where $1 \leq r < |b| = |\overline{G}|$ and $\gcd(|\overline{G}|, r) = 1$. (4 points)

d) Let $f : \mathbf{Z}_{30} \rightarrow \mathbf{Z}_{20}$ be a group homomorphism. Then $f : \mathbf{Z}_{30} \rightarrow \text{Im } f$ is an onto group homomorphism. Since $\text{Im } f$ is a subgroup of \mathbf{Z}_{20} it follows that $|\text{Im } f|$ divides 20. By part a) it follows that $|\text{Im } f|$ divides 30 as well. Thus $|\text{Im } f| = 1, 2, 5, \text{ or } 10$. Now \mathbf{Z}_{20} has a unique subgroup of each of these orders, and these are cyclic. Since cyclic groups of orders 1, 2, 5, and 10 have 1, 1, 4, and 4 generators respectively, there are $1 + 1 + 4 + 4 = 10$ such homomorphisms by part c). (4 points)

3. (12 points total) a) $1 = 1 \cdot 1$ means $1 \in G$. (1 points) Suppose that $r \in G$. Then there is an $r' \in R$ such that $rr' = 1 = r'r$. As $r'r = 1 = rr'$ it follows that $r' \in G$. (2 points) Thus r has an inverse in G which is r' .

To show closure let $r_1, r_2 \in G$. Then there are $r'_1, r'_2 \in R$ such that $r_1 r'_1 = 1 = r'_1 r_1$ and $r_2 r'_2 = 1 = r'_2 r_2$. The equations $r_1 r'_1 = 1$ and $r_2 r'_2 = 1$

imply $(r'_2 r'_1)(r_1 r_2) = 1$ as

$$(r'_2 r'_1)(r_1 r_2) = r'_2 (r'_1 r_1) r_2 = r'_2 1 r_2 = r'_2 r_2 = 1.$$

Therefore the equations $r'_1 r_1 = 1$ and $r'_2 r_2 = 1$ imply $(r_2 r_1)(r'_1 r'_2) = 1$. We have shown that $(r'_2 r'_1)(r_1 r_2) = 1 = (r_2 r_1)(r'_1 r'_2)$. Thus $r_1 r_2 \in G$. (**2 points**)

Since multiplication in R is associative multiplication in G is as well. Thus G is a group under the multiplication of R .

b) $G = \text{GL}(n, \mathbf{R})$. (**2 points**)

c) We show that $G = U(n)$. Note that the multiplication of \mathbf{Z}_n is commutative. Thus the condition $r \cdot r' = 1 = r' \cdot r$ is equivalent to $r \cdot r' = 1$.

Let $r \in G$. Then there is an $r' \in \mathbf{Z}_n$ such that $r \cdot r' = 1$. This means $rr' = qn + 1$ for some $q \in \mathbf{Z}$. Thus $\text{gcd}(n, r) = 1$. By definition $r \in U(n)$.

Conversely, suppose $r \in U(n)$. Then $\text{gcd}(r, n) = 1$. Therefore $rr'' + q''n = 1$ for some $r'', q'' \in \mathbf{Z}$. Write $r'' = q'n + r'$, where $q', r' \in \mathbf{Z}$ and $0 \leq r' < n$. Then $r(q'n + r') + q''n = 1$, or equivalently $rr' = 1 + qn$, where $q = -(rq' + q'')n$. Thus $r \cdot r' = 1$ and consequently $r \in G$. (**5 points**)