

Solutions to Homework Assignment 3

Daniel Mathews

October 20, 2004

Section 3.1, Problem 18.

- (i) The order of σ^4 is 2 as $\sigma^4 \neq 1$ but $\sigma^8 = 1$. By Lagrange's theorem $|\bar{G}| = |G|/|\langle \sigma^4 \rangle| = 16/2 = 8$.
- (ii) Each element of G can be written in the form $\tau^a\sigma^b$ where $0 \leq a \leq 1$ and $0 \leq b \leq 7$. But $\bar{\sigma}^4 = 1$, and thus $\bar{\tau}^a\bar{\sigma}^b = \bar{\tau}^a\bar{\sigma}^{b-4}$. So the elements of \bar{G} are precisely $\bar{\tau}^a\bar{\sigma}^b$ where $0 \leq a \leq 1$ and $0 \leq b \leq 3$.
- (iii) Obviously the order of 1 is 1. The order of $\bar{\sigma}$ is 4, since $\bar{\sigma}^4 = 1$ but no lesser power of $\bar{\sigma}$ is 1. This is also the order of $\bar{\sigma}^{-1} = \bar{\sigma}^3$. The order of $\bar{\sigma}^2$ is 2. And the order of all $\bar{\tau}\bar{\sigma}^b$ is 2, as clearly no such element is the identity, and using the relation $\bar{\sigma}\bar{\tau} = \tau\bar{\sigma}\bar{\sigma}^3$ we may obtain $(\bar{\tau}\bar{\sigma}^b)^2 = \bar{\tau}\bar{\sigma}^b\bar{\tau}\bar{\sigma}^b = \bar{\tau}^2\bar{\sigma}^{3b}\bar{\sigma}^b = \bar{\tau}^2\bar{\sigma}^{4b} = 1$.
- (iv) First we have $\bar{\sigma}\bar{\tau} = \bar{\tau}\bar{\sigma}^3$. Second we have $\bar{\tau}\bar{\sigma}^{-2}\bar{\tau} = \bar{\tau}\bar{\sigma}^2\bar{\tau} = \bar{\tau}\bar{\tau}\bar{\sigma}^6 = \bar{\sigma}^2$. Third we have $\bar{\tau}^{-1}\bar{\sigma}^{-1}\bar{\tau}\bar{\sigma} = \bar{\tau}\bar{\sigma}^3\bar{\tau}\bar{\sigma} = \bar{\tau}\bar{\tau}\bar{\sigma}^9\bar{\sigma} = \bar{\sigma}^2$.
- (v) The group \bar{G} is generated by $\bar{\sigma}$ of order 4 and $\bar{\tau}$ of order 2, with $\bar{\sigma}\bar{\tau} = \bar{\tau}\bar{\sigma}^3 = \bar{\tau}\bar{\sigma}^{-1}$. Thus \bar{G} satisfies all the relations of D_8 , and there is a homomorphism $D_8 \rightarrow \bar{G}$. As the two groups have the same finite order this must be an isomorphism.

Section 3.1, Problem 25.

- (i) If $N \trianglelefteq G$ then for any $g \in G$ we have $gNg^{-1} = N$, so in particular $gNg^{-1} \subseteq N$. Conversely suppose for all $g \in G$ we have $gNg^{-1} \subseteq N$. Take $x \in G$. By our hypothesis, taking $g = x$, we have $xNx^{-1} \subseteq N$. But also by our hypothesis with $g = x^{-1}$, we have $x^{-1}Nx \subseteq N$ so $N \subseteq xNx^{-1}$. Thus $xNx^{-1} = N$ and $N \trianglelefteq G$.
- (ii) With $g \in GL_2(\mathbb{Q})$ as given and $x \in N$, let

$$x = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

where $n \in \mathbb{Z}$. Then

$$gNg^{-1} = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix} \in N$$

so $gNg^{-1} \subseteq N$. However g does not normalize N . For if $gNg^{-1} = N$ then there exists $x \in N$ such that

$$gxg^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

But from above we see the top-right entry of gxg^{-1} is even. So $gNg^{-1} \neq N$.

Section 3.1, Problem 41.

Given a group G , N is defined as the group generated by *commutators*, i.e. elements of the form $x^{-1}y^{-1}xy$ where $x, y \in G$. Any $n \in N$ can thus be written as a product of commutators, and inverses of commutators. But the inverse of a commutator is another commutator: $(x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx$. Thus n can be written as a product of commutators:

$$n = a_1^{-1}b_1^{-1}a_1b_1a_2^{-1}b_2^{-1}a_2b_2 \cdots a_r^{-1}b_r^{-1}a_rb_r.$$

To show $N \trianglelefteq G$, we show for all $g \in G$, $gNg^{-1} \subseteq N$. (This is enough by problem 25 above.) So take $g \in G$ and $n \in N$ of the form above. Then

$$\begin{aligned} gng^{-1} &= ga_1^{-1}b_1^{-1}a_1b_1a_2^{-1}b_2^{-1}a_2b_2 \cdots a_r^{-1}b_r^{-1}a_rb_rg^{-1} \\ &= ga_1^{-1}g^{-1}gb_1^{-1}g^{-1}ga_1g^{-1}gb_1g^{-1} \cdots ga_r^{-1}g^{-1}gb_r^{-1}g^{-1}ga_rg^{-1}gb_rg^{-1} \\ &= [(ga_1g^{-1})^{-1}(gb_1g^{-1})^{-1}(ga_1g^{-1})(gb_1g^{-1})] \cdots [(ga_rg^{-1})^{-1}(gb_rg^{-1})^{-1}(ga_rg^{-1})(gb_rg^{-1})] \in N, \end{aligned}$$

as it is a product of commutators. So $gNg^{-1} \subseteq N$ as required.

Section 3.2, Problem 6.

Suppose $H \leq G$ and $g \in G$, and the right coset Hg is equal to some left coset of H in G . As the left cosets partition G , Hg intersects only one left coset. But as H is a group, $1 \in H$ and hence $g = 1g \in Hg$. Similarly $g \in gH$. So Hg intersects the left coset gH . But then Hg cannot intersect any other left coset, so $Hg = gH$. Thus $gHg^{-1} = H$ and $g \in N_G(H)$.

Section 3.2, Problem 9.

G is a finite group, p and prime dividing $|G|$, and S is the set of p -tuples (x_1, \dots, x_p) where $x_i \in G$ and $x_1 \cdots x_p = 1$.

- (i) If $x_1, \dots, x_{p-1} \in G$ then there is precisely one element x_p for which $(x_1, \dots, x_p) \in S$, namely $x_p = (x_1 \cdots x_{p-1})^{-1}$. Thus $|S|$ is the number of $p-1$ -tuples of elements of G , namely $|G|^{p-1}$.
- (ii) If $(x_1, \dots, x_p) \in S$ then a cyclic permutation is of the form $(x_i, x_{i+1}, \dots, x_p, x_1, \dots, x_{i-1})$. Clearly all $x_i \in G$, and $x_1 \cdots x_p = 1$. Multiplying on the left by x_1^{-1} and then on the right by x_1 gives $x_2x_3 \cdots x_px_1 = 1$. Repeating this process we see $x_i \cdots x_px_1 \cdots x_{i-1} = 1$ also.
- (iii) It's clear that $\alpha \sim \alpha$ since the identity permutation is a cyclic permutation. Similarly, $\alpha \sim \beta$ iff $\beta \sim \alpha$ as the inverse of a cyclic permutation is another cyclic permutation. And if $\alpha \sim \beta, \beta \sim \gamma$ then $\alpha \sim \gamma$ as the composition of two cyclic permutations is another cyclic permutation.

- (iv) Suppose $\alpha = (x_1, \dots, x_p)$ forms an entire equivalence class. Then (x_2, \dots, x_p, x_1) lies in the same equivalence class, so must equal α . Thus $x_1 = x_2, x_2 = x_3$, up to $x_p = x_1$. So $\alpha = (x, x, \dots, x)$ and by definition of S , $x^p = 1$. Conversely, it is clear that any cyclic permutation of (x, x, \dots, x) is itself, so forms an entire equivalence class.
- (v) Given $\alpha = (x_1, \dots, x_p)$, denote by α_i the result of shifting the elements around i places: so $\alpha_0 = \alpha$ and $\alpha_i = (x_{i+1}, \dots, x_p, x_1, \dots, x_i)$. There is some smallest positive d such that $\alpha_d = \alpha_0$. Then we see $\alpha_{d+1} = \alpha_1$, and in general, if $m \equiv n$ modulo d then $\alpha_m = \alpha_n$. Thus for any integer n , α_n is equal to precisely one of $\alpha_0, \dots, \alpha_{d-1}$, accordingly as $n \equiv 0, \dots, d-1$ modulo d , and the size of the equivalence class of α is precisely d . As d was chosen to be the least positive integer such that $\alpha_d = 1$, we see that $\alpha_n = \alpha_0$ if and only if $d|n$.
- Now obviously if we shift everything around p places, everything returns to its starting place, so $\alpha_p = 1$. Thus $d|p$ and as p is prime, $d = 1$ or p . Now S is partitioned into equivalence classes, all of which have size 1 or p . Let there be k classes of size 1 and d classes of size p . Then $|S| = |G|^{p-1} = k + pd$.
- (vi) From part (d) above, $(1, 1, \dots, 1)$ is an equivalence class of size 1, so $k \geq 1$. But we have $|G|^{p-1} = k + pd$, and p divides $|G|$, therefore $p|k$. Since $k \geq 1$ we must actually have $k \geq p \geq 2$. In particular there is at least one more equivalence class of size 1. From part (d) such an equivalence class is of the form (x, \dots, x) where $x^p = 1$, and it must be different from $(1, \dots, 1)$. Hence there is a non-identity element $x \in G$ such that $x^p = 1$.

Section 3.3, Problem 3.

Let $H \trianglelefteq G$ with $|G : H| = p$ for p prime, and let $K \leq G$. Since $H \trianglelefteq G$ we have for any $g \in G$, $gHg^{-1} = H$. So if $h \in H$ and $g \in G$, then $ghg^{-1} = h' \in H$. In particular, if $g \in G$ and $h \in H$, then $gh = h'g$ for some $h' \in G$.

Now consider the set HK . This forms a subgroup of G . For if $hk \in HK$ where $h \in H, k \in K$, then $(hk)^{-1} = k^{-1}h^{-1} = h'k^{-1}$, for some $h' \in H$, by the remark above (taking $g = k^{-1}$). And if $h_1k_1, h_2k_2 \in HK$ then $h_1k_1h_2k_2 = h_1h_2k_1k_2 \in HK$ by the same remark. Thus we have the inclusions

$$H \leq HK \leq G.$$

We use the result that if $A \leq B \leq C$ then $|C : A| = |C : B||B : A|$. So we have $p = |G : H| = |G : HK||HK : H|$. Since p is prime we either have $|HK : H| = 1$, $|G : HK| = p$ or $|G : HK| = 1$, $|HK : H| = p$. A subgroup of order 1 is just the group itself! We consider the two cases separately.

First case: $|HK : H| = 1$ so $HK = H$. Let $k \in K$, then $k = 1k \in HK = H$. So $K \subseteq H$. As both are groups we have $K \leq H$.

Second case: $|G : HK| = 1$ so $G = HK$. In this case, since $H \trianglelefteq G$ we have $H \trianglelefteq HK$. Actually $HK = KH$ for if we take $kh \in KH$ then by the remark above $kh = h'k \in HK$, so $KH \subseteq HK$. Similarly $HK \subseteq KH$ so $HK = KH$.

Anyway, we we may form the quotient HK/H and by the second isomorphism theorem

$$\frac{HK}{K} \cong \frac{KH}{H} \cong \frac{K}{K \cap H}.$$

Thus $|K : K \cap H| = |H : HK| = p$.

Section 3.3, Problem 4.

We have $C \trianglelefteq A$, $D \trianglelefteq B$. Then $C \times D \leq A \times B$; we show it is a normal subgroup. Take $(c, d) \in C \times D$ and $(a, b) \in A \times B$. Then $(a, b)(c, d)(a, b)^{-1} = (aca^{-1}, bdb^{-1}) \in (C, D)$ by normality of C and D . So $(a, b)(C \times D)(a, b)^{-1} \subseteq C \times D$. By an earlier problem this is sufficient to prove $C \times D \trianglelefteq A \times B$.

The normal subgroups $C \trianglelefteq A$, $D \trianglelefteq B$ induce natural quotient maps $A \rightarrow A/C$, $B \rightarrow B/D$. Taking these maps coordinate-wise, we obtain a map $\phi : A \times B \rightarrow (A/C) \times (B/D)$, defined by $\phi(a, b) = (aC, bD)$. This is a homomorphism as $\phi((a_1, b_1)(a_2, b_2)) = \phi(a_1a_2, b_1b_2) = (a_1a_2C, b_1b_2D) = (a_1C, b_1D)(a_2C, b_2D) = \phi(a_1, b_1)\phi(a_2, b_2)$. It is clearly surjective, as we can obtain any $(aC, bD) \in (A/C) \times (B/D)$ as the image of (a, b) . We compute the kernel: if $\phi(a, b) = (1C, 1D)$ then $a \in C, b \in D$, and conversely if $a \in C, b \in D$ then $\phi(a, b) = (1C, 1D)$. Thus $\ker \phi = C \times D$ and by the first isomorphism theorem we obtain the isomorphism

$$\frac{A \times B}{C \times D} \cong \frac{A \times B}{\ker \phi} \cong \text{Image } \phi \cong \frac{A}{C} \times \frac{B}{D}.$$