Solutions of Assignment 10
Basic Algebra I

November 25, 2004

Solution of the problem 1. Let $|a| = m,\ |bab^{-1}| = n$. Since

$$\begin{aligned}(bab^{-1})^m &= (bab^{-1})(bab^{-1})\cdots(bab^{-1})\\ &= ba^mb^{-1}\\ &= b1b^{-1}\\ &= 1,\end{aligned}$$

we have $n \leq m$. Conversely, since

$$\begin{aligned}a^n &= b^{-1}ba^nb^{-1}b\\ &= b^{-1}(bab^{-1})^nb\\ &= b^{-1}1b\\ &= 1,\end{aligned}$$

we have $m \leq n$. Thus $m = n$.

Solution of the problem 2. Recall A non-empty subset H of a group G is a subgroup iff it satisfies the following property:

$$\forall h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H. \qquad (\star)$$

Now back to our problem, we check that $H = H_1 \cap H_2$ satisfies $(\star)$: Take $h_1, h_2 \in H$. So, $h_1, h_2 \in H_1$; $h_1, h_2 \in H_2$. Since both H_1 and H_2 are assumed to be subgroups of G, then $(\star)$ tells us that

$$h_1h_2^{-1} \in H_1, \quad h_1h_2^{-1} \in H_2.$$

Therefore $h_1h_2^{-1} \in H$.

For the union, we shall prove the following:

$H_1 \cup H_2$ is a subgroup of G iff either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Proof Sufficiency is clear. So, suppose that $H_1 \cup H_2$ is a subgroup of G, and, on the contrary, assume that $H_1 \not\subset H_2$ and that $H_2 \not\subset H_1$. These in return imply that

$$\exists h_1 \in H_1, s.t.\ h_1 \notin H_2; \quad \exists h_2 \in H_2, s.t.\ h_2 \notin H_1.$$

Since $h_1h_2 \in H_1 \cup H_2$ (why?), then we would have either $h_1h_2 \in H_1$ or $h_1h_2 \in H_2$, and both are impossible (why?). Done.

Solution of the problem 3. Let $|a| = m$. By Lagrange's theorem, $m \mid n$. So,

$$a^n = (a^m)^{\frac{n}{m}} = 1^{\frac{n}{m}} = 1.$$

For the second part, if $a \equiv 0 \pmod p$, then it is evident that

$$p \mid a(a^{p-1} - 1) = a^p - a.$$

And if $a \not\equiv 0 \pmod p$, then $a \in \mathbb{Z}_p^\times$, and since $\mathbb{Z}_p^\times$ is a group of order $p-1$, by what we proved above, $a^{p-1} = 1$ (in $\mathbb{Z}_p^\times$), so

$$p \mid a(a^{p-1} - 1) = a^p - a.$$

Solution of the problem 4. We verify that $Z(S)$ satisfies $(\star)$ in the solution of problem 2: Let $a, b \in Z(S)$. So, $as = sa,\ bs = sb$ for $s \in S$. First note that $sb^{-1} = b^{-1}bsb^{-1} = b^{-1}sbb^{-1} = b^{-1}s$. Therefore

$$(ab^{-1})s = ab^{-1}s = asb^{-1} = sab^{-1} = s(ab^{-1}),$$

hence $ab^{-1} \in Z(S)$.

Solution of the problem 5. Define $\phi : G_1 \longrightarrow G_2,\ \phi(x) = \ln(x)$. ϕ is clearly bijective. Also note that

$$\phi(xy) = \ln(xy) = \ln(x) + \ln(y) = \phi(x) + \phi(y).$$

So, ϕ is homomorphism, hence an isomorphism.

Solution of the problem 6. Let $|a| = m,\ |f(a)| = n$. Since f is a homomorphism, we have

$$f(a)^m = f(a^m) = f(1_{G_1}) = 1_{G_2}.$$

So, $n \leq m$. If f is also injective, we have

$$f(a^n) = f(a)^n = 1_{G_2} = f(1_{G_1}).$$

So, $a^n = 1_{G_1}$, since f is injective. Thus $m \leq n$ and we are done.

Solution of the problem 7. Note that:

(i) G is closed under multiplication (check this);

(ii) G contains the identity element 1 (clear);

(iii) G contains the inverse of all its elements:

$$(\pm 1)^{-1} = \pm 1, \quad (\pm i)^{-1} = \mp i, \quad (\pm j)^{-1} = \mp j, \quad (\pm k)^{-1} = \mp k.$$

Hence G is a (sub)group of the multiplicative group of non-zero elements of H.

For the second part, enough to see that the dihedral group D_4 has two elements of order 4, namely r_1 and r_3, whereas in the group G above, there are six elements of order 4, namely $\pm i, \ \pm j, \ \pm k$. So, $G \not\cong D_4$.

Extra Credit

Solution of the problem 9. Let $V = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(1,0),(0,1),(1,1)\} = \{o, e_1, e_2, e_3\}$, where $o = (0,0), e_1 = (1,0), e_2 = (0,1), e_3 = (1,1)$. We will view V as a vector space of dimension 2 over the field $\mathbb{Z}_2$. Fix the basis $\{e_1, e_2\}$ for V. Now each matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_2)$$

may be viewed as a bijective linear transformation from V into itself (by multiplication from left to e_i's). Each $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ permutes e_1, e_2, e_3. For example

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} e_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e_1,$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} e_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = e_3,$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} e_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e_2.$$

So, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ can be corresponded to the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

In general, we can define a well-defined map, ψ say, from the group $GL_2(\mathbb{Z}_2)$ into the group S_3:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix},$$

where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} e_i = e_{\sigma(i)} \quad (1 \le i \le 3).$$

ψ is clearly an injective group homomorphism (check this). On the other hand, since $|S_3| = |GL_2(\mathbb{Z}_2)| = 6$, we conclude that ψ is also onto, hence an isomorphism.

Solution of the problem 10. Let G be a group, and let $a, b \in G$. b is said to be *conjugate* to a if $b = gag^{-1}$ for some $g \in G$. Notice that

(i) Every a is conjugate to itself: $a = 1a1^{-1}$;

(ii) If b is conjugate to a, then a is also conjugate to b:

$$b = gag^{-1} \Rightarrow a = g^{-1}b(g^{-1})^{-1};$$

(iii) If b is conjugate to a, and if c is conjugate to b, then c is also conjugate to a:

$$b = g_1 a g_1^{-1},\ c = g_2 b g_2^{-1} \Rightarrow c = (g_2 g_1) a (g_2 g_1)^{-1}.$$

So, conjugacy is an equivalence relation in G. Denote the *conjugacy class* of $a \in G$ by $cl[a]$:

$$cl[a] := \{gag^{-1} :\ g \in G\}.$$

Now suppose that $N \rhd G$, i.e., N is a normal subgroup of G. Given any $a \in N$, it is obvious that $cl[a] \subseteq N$ (why?). Thus N is the disjoint union of the conjugacy classes of its elements. Conversely, if a subgroup of G is a union of some conjugacy classes in G, that subgroup is clearly normal. So, one way to find all normal subgroups of G is to look at those unions of conjugacy classes in G which constitute a subgroup.

To determine the conjugacy classes in the symmetric group S_n, we will exploit the following useful fact:

Permutations $\alpha, \beta \in S_n$ are conjugate iff the have the **same cyclic structure**, i.e., iff their complete factorization into disjoint cycles have the same number of r-cycles for each r.

Example Let

$$\alpha = (2\ 3\ 1)(4\ 5)(6);$$
$$\beta = (5\ 6\ 2)(3\ 1)(4);$$
$$\gamma = (2\ 3\ 1)(4\ 5\ 6).$$

α and β are conjugate, since they have the same cyclic structure. In fact the permutation $\delta = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,5\,6\,3\,1\,4 \end{pmatrix}$ does what we want: $\delta\alpha\delta^{-1} = \beta$ (check this). In complete contrast, α and γ are not conjugate, because they don't have the same cyclic structure.

Using the above fact, now listing the set of all conjugacy classes in S_4 is an easy(!) task:

$$C_1 = \{(1)\};$$
$$C_2 = \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\};$$
$$C_3 = \{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\};$$
$$C_4 = \{(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\};$$
$$C_5 = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Examining all the possibilities, one can find all the normal subgroups of S_4:

$$\{1\} = C_1;\ V = C_1 \cup C_5;\ A_4 = C_1 \cup C_3 \cup C_5;\ S_4 = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5.$$

As for S_5, the following is the complete list of all conjugacy classes:

$$cl[(1)]; cl[(1\ 2)];\ cl[(1\ 2\ 3)]; cl[(1\ 2\ 3\ 4)];$$

$$cl[(1\ 2\ 3\ 4\ 5)];\ cl[(1\ 2)(3\ 4)];\ cl[(1\ 2\ 3)(4\ 5)].$$

And finally, one can find all normal subgroups of S_5. Here you are:

$$\{1\};\quad A_5;\quad S_5.$$

Conclusion A_5 is the only proper non-trivial normal subgroup of S_5. **In fact, this holds for any** $n \neq 4$.