Some solutions and some comments
September 29, 2008

Homework # 1

Section 0.3

4. Compute the remainder when 37^{100} is divided by 29.

   This question asks you to determine 37^{100} mod 29, where 29 is a prime. Notice that $\varphi(29) = 28 = |(\mathbb{Z}/29\mathbb{Z})^*|$. Thus,

$$\begin{aligned} 37^{100} &\equiv 37^{28\cdot 3+16} \bmod 29 \\ &\equiv 37^{16} \bmod 29 \\ &\equiv 8^{16} \bmod 29 \\ &\equiv 23 \bmod 29. \end{aligned}$$

5. Compute the last two digits of 9^{1500}.

   Here you want to compute 9^{1500} mod 100, so we first compute that $\varphi(100) = 40$.

$$\begin{aligned} 9^{1500} \bmod 100 &\equiv 9^{20} \bmod 100 \\ &\equiv 3^{40} \bmod 100 \\ &\equiv 1 \bmod 100. \end{aligned}$$

   It follows that the last two digits are 01.

Homework #2

Section 2.1

6. Give an example of a non-Abelian group G in which the set of torsion elements of G is not a subgroup.

   Example: Consider the group $\mathrm{GL}_2(\mathbb{R})$.

   There are lots of examples in this group. For instance, $|\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}| = 3$, $|\begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}| = 4$, but their product is not a torsion element. (Check this.)

Section 2.2

4. For each of S_3, D_8, and Q_8 compute the centralizers of each element and find the center of each group. Does Lagrange's theorem help with the computations?

   (a) $S_3 = \{1,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$

$$\begin{aligned} C_{S_3}(\{1\}) &= S_3 \\ C_{S_3}(\{1\ 2\}) &= \langle(1\ 2)\rangle \\ C_{S_3}(\{1\ 3\}) &= \langle(1\ 3)\rangle \\ C_{S_3}(\{2\ 3\}) &= \langle(2\ 3)\rangle \\ C_{S_3}(\{(132)\}) &= \langle(123)\rangle = C_{S_3}(\{(132)\}). \end{aligned}$$

(b) $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

$$\begin{aligned}
C_{Q_8}(\{1\}) &= Q_8 \\
C_{Q_8}(\{-1\}) &= Q_8 \\
C_{Q_8}(\{i\}) &= \{1, -1, i, -i\} = \langle i \rangle \\
C_{Q_8}(\{j\}) &= \{1, -1, j, -j\} = \langle j \rangle \\
C_{Q_8}(\{k\}) &= \{1, -1, k, -k\} = \langle k \rangle \\
C_{Q_8}(\{-i\}) &= \{1, -1, i, -i\} = \langle i \rangle \\
C_{Q_8}(\{-j\}) &= \{1, -1, j, -j\} = \langle j \rangle \\
C_{Q_8}(\{-k\}) &= \{1, -1, k, -k\} = \langle k \rangle
\end{aligned}$$

(c) $D_8 = \{1,\ r,\ r^2,\ r^3,\ s,\ sr,\ sr^2,\ sr^3\}$

$$\begin{aligned}
C_{D_8}(\{1\}) &= D_8 \\
C_{D_8}(\{r\}) &= \{1,\ r,\ r^2,\ r^3\} = \langle r \rangle \\
C_{D_8}(\{r^2\}) &= \{1,\ r,\ r^2,\ r^3,\ s,\ sr,\ sr^2,\ sr^3\} = D_8 \\
C_{D_8}(\{r^3\}) &= \{1,\ r,\ r^2,\ r^3\} = \langle r \rangle \\
C_{D_8}(\{s\}) &= \{1,\ r^2,\ s,\ sr^2\} = \langle s,\ r^2 \rangle \\
C_{D_8}(\{sr\}) &= \{1,\ r^2,\ sr,\ sr^3\} = \langle rs,\ r^2 \rangle \\
C_{D_8}(\{sr^2\}) &= \{1,\ r^2,\ s,\ sr^2\} = \langle s,\ r^2 \rangle \\
C_{D_8}(\{sr^3\}) &= \{1,\ r^2,\ sr,\ sr^3\} = \langle rs,\ r^2 \rangle
\end{aligned}$$

(d) $D_{16} = \{1,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7,\ s,\ sr,\ sr^2,\ sr^3,\ sr^4,\ sr^5,\ sr^6,\ sr^7\}$ — really for problem 6 in Section 2.5

$$\begin{aligned}
C_{D_{16}}(\{1\}) &= D_{16} \\
C_{D_{16}}(\{r\}) &= \{1,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7\} = \langle r \rangle \\
C_{D_{16}}(\{r^2\}) &= \{1,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7\} = \langle r \rangle \\
C_{D_{16}}(\{r^3\}) &= \{1,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7\} = \langle r \rangle \\
C_{D_{16}}(\{r^4\}) &= \{1,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7,\ s,\ sr,\ sr^2,\ sr^3,\ sr^4,\ sr^5,\ sr^6,\ sr^7\} = D_{16} \\
C_{D_{16}}(\{r^5\}) &= \{1,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7\} = \langle r \rangle \\
C_{D_{16}}(\{r^6\}) &= \{1,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7\} = \langle r \rangle \\
C_{D_{16}}(\{r^7\}) &= \{1,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7\} = \langle r \rangle \\
C_{D_{16}}(\{s\}) &= \{1,\ r^4,\ s,\ sr^4\} = \langle s,\ r^4 \rangle \\
C_{D_{16}}(\{sr\}) &= \{1,\ r^4,\ ,\ sr,\ sr^5\} = \langle sr^5,\ r^4 \rangle \\
C_{D_{16}}(\{sr^2\}) &= \{1,\ r^4,\ sr^2,\ sr^6\} = \langle sr^2,\ sr^4 \rangle \\
C_{D_{16}}(\{sr^3\}) &= \{1,\ r^4,\ sr^3,\ sr^7\} = \langle sr^3,\ r^4 \rangle \\
C_{D_{16}}(\{sr^4\}) &= \{1,\ r^4,\ sr^4,\ s\} = \langle s,\ r^4 \rangle \\
C_{D_{16}}(\{sr^5\}) &= \{1,\ r^4,\ sr,\ sr^5\} = \langle sr^5,\ r^4 \rangle \\
C_{D_{16}}(\{sr^6\}) &= \{1,\ r^4,\ sr^2,\ sr^6\} = \langle sr^2,\ r^4 \rangle \\
C_{D_{16}}(\{sr^7\}) &= \{1,\ r^4,\ sr^3,\ sr^7\} = \langle sr^3,\ r^4 \rangle
\end{aligned}$$

6. Let H be a subgroup of G.

   (a) Show that $H \leq N_G(H)$.
   COMMENTS: To establish this, it is enough to show that $H \subseteq N_G(H)$ since we already know that H is a subgroup. (This follows immediately from the definition of $N_G(H)$.) Don't waste your words.

8. Let $G = S_n$, fix an $i \in \{1, 2, \ldots, n\}$ and let $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ (the stabilizer of i). Use group actions to show that G_i is a subgroup of G.

   COMMENTS: Let G act on $A = \{1, \ldots, n\}$ by $\sigma \cdot i = \sigma(i)$. Then by problem 4a in Section 1.7, the stabilizer of any point in A is a subgroup of G. (I.e. once you establish that this is a group action, you are done....)

   It is helpful to notice that G_i acting on A is an action isomorphic to S_{n-1} acting on $A \setminus \{i\}$. This lets us see that $|G_i| = (n-1)!$. Alternatively, just think about G_i; it consists of all permutations of n that don't move i. Thus, it consists of all possible permutations on $A' = \{1, \ldots, i-1, i+1, \ldots, n\}$.

Section 2.3

8. Let $\mathbb{Z}_{48} =< x >$ be a cyclic group of order 48. For which integers a does the map $\phi_a : \bar{1} \mapsto x^a$ extend to an *isomorphism* from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48}?

   Solution: The map ϕ_a above extends to a well-defined homomorphism if, and only if, $(a, 48) = 1$, *i.e.* the generator $\overline{1}$ must be sent to a generator.

   Proof. Define the map ϕ_a by
   $$\phi_a(\overline{m}) = x^{am}, \quad \forall \overline{m} \in \mathbb{Z}/48\mathbb{Z}.$$

   We must show that ϕ_a is well-defined and an isomorphism exactly when a and 48 are relatively prime. Note that if ϕ_a is well-defined, then it will also be a homomorphism since then
   $$\phi_a(\overline{mn}) = x^{aman} = x^{am}x^{an} = \phi_a(\overline{m})\phi_a(\overline{n}).$$

   To show that ϕ_a is well-defined, suppose that $\overline{m} = \overline{m}' \in \mathbb{Z}/48\mathbb{Z}$. Then $\exists k \in \mathbb{Z}$ so that $m' = m + 48k$. Thus, $\phi_a(\overline{m}') = x^{am'} = x^{a(m+48k)} = x^{am}x^{a48k} = x^{am}$ in Z_{48}. So $\phi_a(m) = \phi_a(m')$, as needed.

9. Let $Z_{36} =< x >$ be a cyclic group of order 36. For which integers a does the map $\psi_a : \bar{1} \mapsto x^a$ extend to a *well-defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ into Z_{36}?

   Comments: The insight for this problem is that $\bar{1}$, the generator of $\mathbb{Z}/48\mathbb{Z}$, must be mapped by ψ_a to an element of order dividing 48 in Z_{36}. Thus, $|x^a| \,\Big|\, 48$. We also know that $|x^a| = \frac{36}{(36,a)}$ in Z_{36}. Putting this together, we have that $\frac{36}{(36,a)} \,\Big|\, 48$. For this to be true, we must have that $3 \mid (36, a)$, or equivalently that $3 \mid a$, since $9 \mid 36$, but $3 \,\|\, 48$.

   Solution: The map ψ_a above extends to a well-defined homomorphism if, and only if, $3 \mid a$.

   Proof. Define the map ψ_a by
   $$\psi_a(\bar{m}) = x^{am}, \quad \forall \bar{m} \in \mathbb{Z}/48\mathbb{Z}.$$

Let $\bar{m} = \bar{m}' \in \mathbb{Z}/48\mathbb{Z}$. Then, there is an integer k so that $m' = m + 48k$. We have

$$\begin{aligned}
&\psi_a(\bar{m}) = \psi_a(\bar{m}') \\
\iff\ & x^{am} = x^{am'} \\
\iff\ & x^{am} = x^{a(m+48k)} \\
\iff\ & x^{am} = x^{am}x^{48ka} \\
\iff\ & 1 = x^{48ka} \text{ in } Z_{36} \text{ by left cancellation} \\
\iff\ & 36 \,\Big|\, 48ka \\
\iff\ & 36 \,\Big|\, 48a
\end{aligned}$$

since x has order 36 in Z_{36} and k depended on the representative m' for $\bar{m}$ chosen. Finally, $36 \,\Big|\, 48a \iff 3 \,\Big|\, a$.