Shashank Singh
sss1@andrew.cmu.edu
21-373 Algebraic Structures, Fall 2011
Assignment 4
Due: Friday, October 7

Exercise 22: Lemma: If G is a finite group and $p = |G|$, the order of G, is prime, then G is cyclic.

Proof: Let $g \in G$, with $g \neq e$ (such a G exists, since p is prime and thus $p > 1$). Since the order of g divides p and is greater than 1, it must be p, and so, $\forall i, j \in \mathbb{N}$ with $i < j < p$, $g^i \neq g^j$. Therefore, the p distinct elements $e, g, g^2, g^3, \ldots, g^{p-1}$ are precisely the elements of G and G is cyclic. ■

As a consequence of the above lemma, a subgroup of E_{p^n} of order p is determined by determining a single generator element. If, for some $k_2, k_3, \ldots, k_n, l_2, l_3, \ldots, l_n \in \mathbb{Z}_n$, letting $b = 1$, $g_1 = (b, k_2, k_2, \ldots, k_n)$, $g_2 = (b, l_2, l_3, \ldots, l_n)$, then $< g_1 >=< g_2 >$ if and only if $k_1 = l_1, k_2 = l_2, \ldots, k_n = l_n$. This follows from the fact that $k_i^n = l_i^n \ \forall n \in \mathbb{N}$ if and only if $k_i = l_i$. Thus, choosing values for $k_2, k_3, \ldots, k_n$ from the p values in $\mathbb{Z}_p$, there are p^{n-1} subgroups of the form of g_1. The same reasoning holds if we let $b = 0$, with the exception that e does not generate a subgroup of order p. Thus, there are $2 * p^{n-1} - 1$ subgroups of E_{p^n} of order p.

Exercise 23: Let G be a finite group, and let n be the order of G. Then, since, $\forall g \in G$, the order of g must divide the order of G, n is a natural number such that $\forall g \in G$, $g^n = e$, so $\exists$ a minimal $k \in \mathbb{N}$ such that, $\forall g \in \mathbb{G}$, $g^k = e$ (i.e., k is the exponent of G).

Note that k is not necessarily the order of any element in G; consider, for instance, the symmetric group S_3. The exponent of S_3 is 6, but no element of S_3 has order greater than 3.

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots$ Then, $|G| = |\mathcal{P}(\mathbb{N})|$ (the mapping $f : \mathbb{G} \to \mathcal{P}(\mathbb{N})$ such that, $\forall g = (g_1, g_2, g_3, \ldots) \in G$, $f(g) = \{n \in \mathbb{N} : g_n = 1\}$ gives a simple bijection), but the order of any element $g \in G$ is 1 or 2, so that the exponent of G is 2. Thus, there exist infinite groups of finite exponent. ■

Exercise 24: Let G be an Abelian group, let $p \in \mathbb{N}$ be prime, let $G^p = \{g^p : g \in G\}$, and let $G_p = \{g \in G : g^p \in G\}$. Clearly, by their definition, and the closure of G under its group operation, $G^p \subseteq G$ and $G_p \subseteq G$. Furthermore, clearly, $e \in G^p$ and $e \in G_p$, since $e^p = e$, so $G^p \neq \emptyset$ and $G_p \neq \emptyset$. Suppose $a, b \in G^p$. Then, $\exists g_1, g_2 \in G$, such that $g_1^p = a, g_2^p = b$. Thus, $g_1 g_2^{-1} \in G$, so, since G is Abelian and thus $\left(g_1 g_2^{-1}\right)^p = g_1^p \left(g_2^p\right)^{-1} = ab^{-1}$, $ab^{-1} \in G^p$. Suppose, on the other hand, that $g_1, g_2 \in G_p$, so that $g_1^p = g_2^p = e$. Then, since G is Abelian, $\left(g_1 g_2^{-1}\right)^p = g_1^p \left(g_2^p\right)^{-1} = ee^{-1} = e$, so $g_1 g_2^{-1} \in G_p$. Thus, $G^p \leq G$ and $G_p \leq G$. ■

Let G, H, K be groups, with $G = H \times K$, and let $p \in \mathbb{N}$ be prime.

Suppose $g \in H^p \times K^p$, so that $\exists h_1 \in H^p, k_1 \in K^p$, such that $g = (h_1, k_1)$. Then, for some $h_0 \in H, k_0 \in K$, $h_1 = h_0^p$ and $k_1 = k_0^p$, so that $g = (h_1, h_1) = (h_0, k_0)^p$. Thus, since $(h_0, k_0) \in G$ and G is a group and consequently closed under its operation, $g \in G$. Suppose, on the other hand, that $g_1 \in G^p$, so that $g_1 = g_0^p$, for some $g_0 \in G$. Since $G = H \times K$, $g_0 = (h_0, k_0)$, for some $h_0 \in H, k_0 \in K$, so that $g_1 = (h_0, k_0)^p = (h_0^p, k_0^p)$. Thus, since $h_0^p \in H^p$ and $k_0^p \in K^p$, $g_1 \in H^p \times K^p$. Therefore, $G^p = H^p \times K^p$.

Suppose $g \in H_p \times K_p$, so that, for some $h \in H, k \in K$ with $h^p = e_H$, $k^p = e_K$ (where e_H, e_K denote the identities of their respective groups), $g = (h, k)$. Since $G = H \times K$, $g \in G$. Furthermore, (e_H, e_K) is the identity of $H \times K$ and thus of G (i.e., $(e_H, e_K) = e$), so, since $g^p = (h, k)^p = (h^p, k^p) = (e_H, e_K) = e$, $g \in G_p$. Suppose, on the other hand, that $g \in G^p$. Then, since $G = H \times K$, $g \in (H \times K)^p$, so $\exists h \in H, k \in K$ such that $g = (h, k)$ and $(h^p, k^p) = (h, k)^p = e = (e_H, e_K)$. Therefore, $h \in H_p, k$, so $g = (h, k) \in H_p \times K_p$. Therefore, $G_p = H_p \times K_p$. ■

Exercise 27: Let G be a group of order pqr, where $p, q, r \in \mathbb{N}$ are primes with $p < q < r$. Let n_p, n_q, n_r denote the number of Sylow-p,-q, and -r subgroups of G, respectively. Suppose, for sake of contradiction, that G is simple. Then, $n_p, n_q, n_r > 1$, since, otherwise, as explained in Remark 11.6 a Sylow-p,-q, or -r

subgroup would be a non-trivial normal subgroup of G. By another of the Sylow theorems, $n_p \cong 1 \pmod{p}$, $n_q \cong 1 \pmod{q}$, and $n_r \cong 1 \pmod{r}$, so that $n_p > p$, $n_q > q$, and $n_r > r > q > p$. Then, since p, q are prime and, by another of the Sylow theorems $n_r | pq$, $n_r = pq$. Similarly, since $n_q | pr$ and $n_p | qr$, $n_q \geq r$ and $n_p \geq q$. Note that, since the Sylow-p subgroups of G are all cyclic (as shown in the proof for Exercise 22), they are disjoint except for the identity (i.e., if G_1, G_2 are two distinct Sylow-p subgroups of G, then $G_1 \cap G_2 = \{e\}$). Furthermore, the same holds for any pair of a Sylow-q subgroups or Sylow-r subgroups, as well as any pair of Sylow-p, Sylow-q, and Sylow-r subgroups. Thus, the number of elements in G is at least

$$\begin{aligned} |\{e\}| + n_r(r-1) + n_q(q-1) + n_p(p-1) &\geq 1 + pq(r-1) + r(q-1) + q(r-1) \\ &> pq(r-1) + r(q-1) \\ &\geq pq(r-1) + pq = pqr. \end{aligned}$$

However, this contradicts the given that G is of order pqr. Thus, G cannot be simple.

Let G be a group of order p^2q, where $p, q \in \mathbb{N}$ are primes with $p < q$. Suppose, for sake of contradiction, that G is simple. As explained previously, since G is simple, letting n_p denote the number of Sylow-p subgroups of G and n_q the number of Sylow-q subgroups of G, $n_p, n_q > 1$, $n_p | q$, $n_q | p^2$, $n_p \cong 1 \pmod{p}$, and $n_q \cong 1 \pmod{q}$, so that $n_q = p^2$ (since $n_q = p$ or $n_q = p^2$, but $n_q > q > p$), $n_p = q$, and thus $q | (p^2 - 1)$. Since q is prime, this implies that $q | (p+1)$ or $q | (p-1)$. The latter is impossible, since $p < q$; the former implies $q = p+1$, for the same reason. Since either p or $p+1$ is even, and both p and q are prime, this is only possible if $p = 2$ and $q = 3$. However, then, there are $(q-1) * n_q = 8$ elements of order q, 1 element of order 1 (the identity), so there are not enough elements to construct the requisite number of Sylow-p subgroups ($n_p = 3$).

Exercise 28: Suppose, for sake of contradiction, that there exists a a simple group G of order 90. As explained in the proof of Exercise 27, by the result of 11.6, since G is simple, if p is prime, the number of Sylow-p subgroups of G, denoted n_p, must be greater than 1 (i.e., $n_p > 1$). Furthermore, by the Sylow theorems, $n_p \cong 1 \pmod{p}$ and $n_p | (90/p)$. Thus, $n_5 \cong 1 \pmod{5}$, $n_5 | 18$, and $n_p > 1$, so $n_p = 6$, and, similarly, it can be seen that $n_3 = 10$. However, since the intersection of different Sylow-p subgroups can contain only the identity, this implies there are $(9-1) * 10 = 80$ elements of order 9, and $(5-1) * 6 = 24$ elements of order 5, which is impossible, since $24 + 80 > 90 = |G|$. Thus, no simple group of order 90 can exist.