**Instructions**: Same rules as usual. Work together, write-up alone, no internet!

(6pts) 1. Consider the 362880 elements in $S_9$.

(a) What are the possible orders of elements in $S_9$. For each possible order, give an example of an element with that order. Explain how you know you have them all.

**Solution:** We know that the order of a cycle is its length, so there are elements of all orders in $\{1, 2, \ldots, 9\}$, namely (1), (12), (123), ..., (123456789). We can also get orders that are least common multiples of the lengths of disjoint cycles. This way we can get 6 (again), 10 as (12)(34567), 14 as (12)(3456789), 12 as (123)(4567), 15 as (123)(45678) and 20 as (1234)(56789). But that is all.

(b) Give an example of an element with order 3 that does not fix any element of $\{1, 2, \ldots, 9\}$.

**Solution:** (123)(456)(789) leaves no element fixed, but has order 3.

(c) What do elements of order 8 look like? Bonus: how many elements of order 8 are there?

**Solution:** The only order 8 elements are the 8-cycles. This is because any set of numbers with least common multiple 8 must include 8 itself.

To count these, not that since we always start a cycle with the smallest number in it, the cycle must start with either a 1 or a 2. If it starts with a 1, there are 8! choices for the rest of the cycle (8 choices for the next number, 7 for the one after that, and so on until we have picked 7 numbers, so this is really $P(8, 7) = 8!/1!$). If it starts with a 2, then there cannot be a 1 in the cycle, so there are 7! ways to finish the cycle. Thus there are $8! + 7! = 45360$ elements with order 8 (which happens to be 1/8 of all cycles in $S_9$).

(8pts) 2. Prove the following basic facts about orders of elements. None of these are particularly difficult, so you should put most of your effort into writing a nice, clean proof of the fact. In each of the following, $a$ is an element of a group $G$.

(a) If $\text{ord}(a) = n$ then for any $r < n$, $a^{n-r} = (a^r)^{-1}$.

**Solution:**

*Proof.* Let $a$ be an element of a group with $\text{ord}(a) = n$, and let $r < n$. Now $a^{n-r} \cdots a^r = a^{n-r+r} = a^n = e$ so $(a^r)^{-1} = a^{n-r}$. □

(b) The order of $a^{-1}$ is the same as the order of $a$.

**Solution:**

*Proof.* Again let $\text{ord}(a) = n$. Now $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$ so we know that $\text{ord}(a^{-1})$ is at most $n$. We must also argue that no smaller $k$ has $(a^{-1})^k = e$. But if there were such a $k < n$, then we would have $(a^k)^{-1} = e$. The only element that has $e$

as an inverse is $e$ itself, so this would say $a^k = e$, a contradiction since $n$ was the least positive such exponent. □

(c) If $a^k = e$ where $k$ is odd, then the order of $a$ is odd.

**Solution:**

*Proof.* Suppose $a^k = e$ for some odd number $k$. This does not mean that $k$ is the order of $a$, but we do know that $k$ will be a multiple of the order of $a$. If $\mathrm{ord}(a)$ were even, then every multiple of that order would be even as well. Since $k$ is an odd multiple of the order, we know the order must be odd as well. □

(d) If $a \neq e$ and $a^p = e$ where $p$ is prime, then $\mathrm{ord}(a) = p$.

**Solution:**

*Proof.* Suppose $a \neq e$ and $a^p = e$ where $p$ is prime. This does not mean that $\mathrm{ord}(a) = p$ right away, just that $p$ is a multiple of $\mathrm{ord}(a)$. But since $p$ is prime, $p$ is only a multiple of 1 and $p$. We know that $\mathrm{ord}(a) \neq 1$ since $a \neq e$. Thus $\mathrm{ord}(a) = p$. □

(12pts) 3. Let $a$ and $b$ be elements of a group $G$ with $\mathrm{ord}(a) = m$ and $\mathrm{ord}(b) = n$.

(a) Assume $a$ and $b$ commute. Let $k = \mathrm{ord}(ab)$ and $p = \mathrm{lcm}(m, n)$. Prove $k$ divides $p$.

**Solution:**

*Proof.* Assume $\mathrm{ord}(ab) = k$. Consider $(ab)^p = a^p b^p$ (since $a$ and $b$ commute). But $p$ is a multiple of $m$ and of $n$ so this means $(ab)^p = a^p b^p = e \cdot e = e$. But this means that $p$ is a multiple of $\mathrm{ord}(ab)$, as needed.

Note you could also prove this from scratch using the division algorithm (which is how we know that the only exponents that give the identity are multiples of the order). □

(b) Assume $m$ and $n$ are relatively prime (i.e., $\gcd(m, n) = 1$). Prove that no power of $a$ is equal to any power of $b$ (other than $e$).

**Solution:**

*Proof.* Suppose that $a^k = b^j$. But then $(a^k)^n = (b^j)^n = (b^n)^j = e^j = e$, and similarly $(b^j)^m = (a^k)^m = (a^m)^k = e^k = e$. This proves that $m$ and $n$ are both multiples of the order of $a^k$ (which is the same as the order of $b^j$). But since the only number that $m$ and $n$ are both multiples of is 1, we have that $a^k = e = b^j$. That is, if any power of $a$ is equal to a power of $b$, then those powers are the identity. □

(c) Use the previous parts to prove that if $a$ and $b$ commute and $m$ and $n$ are relatively prime, then $\mathrm{ord}(ab) = mn$.

**Solution:**

*Proof.* From the previous parts we know that $\mathrm{ord}(ab)$ divides $\mathrm{lcm}(m,n) = mn$, and that no power of $a$ is equal to a power of $b$ (other than $e$). Again let $k = \mathrm{ord}(ab)$. We have $(ab)^k = a^k b^k = e$, or in other words $a^k = b^{-k}$. By part (b), this implies that $a^k = e = b^{-k} = b^k$. But then $k$ is a multiple of both $m$ and $n$, so is also a multiple of $\mathrm{lcm}(m,n)$. The only multiple of $\mathrm{lcm}(m,n)$ that is also a divisor of $\mathrm{lcm}(m,n)$ is $\mathrm{lcm}(m,n)$ itself. Thus $k = mn$. $\square$

(d) Give an example to show that part (a) is not true if $a$ and $b$ do not commute.

**Solution:** For example, $a = (12)$ and $b = (13)$. Then $ab = (132)$ and $\mathrm{ord}(ab) = 3$. However, $\mathrm{lcm}(2,2) = 2$ and 3 does not divide 2.

(4pts) 4. Suppose $G$ is a group and $H$ and $K$ are distinct subgroups both with order the same prime number $p$. Prove that $H \cap K = \{e\}$. Hint: use Lagrange's theorem.

**Solution:** Consider an element $a \in H \cap K$. Since $H$ is a group of order $p$, every element in $H$ (including $a$) must have order dividing $p$, by Lagrange's theorem. Since $p$ is prime, this means $\mathrm{ord}(a) = p$ or $\mathrm{ord}(a) = 1$. If $\mathrm{ord}(a) = p$, then the $p$ different powers of $a$ all belong to $H$, and also to $K$. But since both $H$ and $K$ only have $p$ different elements, this means that $\langle a \rangle = H = K$ and the subgroups are not distinct. Thus we have that $\mathrm{ord}(a) = 1$, so $a = e$. In other words, the only element in both $H$ and $K$ is the identity.

An alternative proof would be to recall that $H \cap K$ is a subgroup of $G$, and since $H \cap K \subseteq H$ also a subgroup of $H$ (and similarly of $K$). Since $H$ has order $p$, we know by Lagrange's theorem that the order of $H \cap K$ is either $p$ or 1. If it is $p$, then $H \cap K = H = K$, contradicting the assumption that $H$ and $K$ are distinct. Thus $|H \cap K| = 1$ so $H \cap K = \{e\}$.