Practice Problem Solutions

1. Despite its appearance, this is a problem dealing exclusively with cosets and not using Lagrange's Theorem. We start with the following observation. Let $a, b \in K$ and suppose that $a(H \cap K) = b(H \cap K)$. Then $a^{-1}b \in H \cap K \leq H$ and so $aH = bH$. It follows that the map

$$\begin{array}{rcl} \{a(H \cap K) \,|\, a \in K\} & \to & \{aH \,|\, a \in H \vee K\} \\ a(H \cap K) & \mapsto & aH \end{array}$$

is well-defined, i.e. does not depend on the choice of coset representative a. Moreover, this map is one-to-one. For if $a, b \in K$ and $aH = bH$ then $a^{-1}b \in H$ and since $a^{-1}b \in K$ we have $a^{-1}b \in H \cap K$ so that $a(H \cap K) = b(H \cap K)$. It follows that the number of cosets in the set on the left above (which is $[K : H \cap K]$) is less than or equal to the number of cosets in the set on the right above (which is $[H \vee K : H]$). That is

$$[K : H \cap K] \leq [H \vee K : H].$$

2. In a recent homework assignment, we showed that the subgroup

$$G = \{\sigma \in S_4 \,|\, \sigma(4) = 4\}$$

is isomorphic to S_3. There's nothing particularly special about the integer 4, and the same technique can be used to show that the three subgroups

$$\{\sigma \in S_4 \,|\, \sigma(i) = i\},$$

$i = 1, 2, 3$ are all also isomorphic to S_3.

3. Let (ab) be a transposition in S_n. If $a = 1$ or $b = 1$ then (ab) is already among $(12), (13), \ldots, (1n)$. So suppose that $a, b \neq 1$. Then, since $a \neq b$, it is trivial to verify that

$$(ab) = (1a)(1b)(1a).$$

It follows that any transposition can be written using only the transpositions $(12), (13), \ldots, (1n)$, and since any permutation can be written as a product of transpositions, that any element of S_n can be written using only the transpositions $(12), (13), \ldots, (1n)$.

4. (a) Suppose that $\sigma \in S_n$ is a 3-cycle. Then σ has order 3. If $\sigma \notin H$ then, since $\sigma = (\sigma^2)^2$, we must have $\sigma^2 \notin H$ as well. That is, $\sigma H \neq H$ and $\sigma^2 H \neq H$. But H has index 2 and so only has two cosets in S_n. Therefore it must be that $\sigma H = \sigma^2 H$. But this can only happen if $\sigma = \sigma^{-1}\sigma^2 \in H$, which is a contradiction! Therefore it must be the case that $\sigma \in H$. Since σ was an arbitrary 3-cycle, we conclude that H contains all 3-cycles.

(b) If $H \leq S_n$ has index 2, then part (a) tells us that H contains every 3-cycle. Since every element of A_n is a product of 3-cycles, it follows that $A_n \leq H$. But $[S_n : A_n] = 2 = [S_n : H]$ and so $H = A_n$ by the following exercise.

5. We must make the additional assumption that G is *finite*. In this case, Lagrange's Theorem tells us that

$$\frac{|G|}{|H|} = [G : H] = [G : K] = \frac{|G|}{|K|}$$

so that $|H| = |K|$. Since $H \leq K$ and the two sets are finite, we conclude immediately that $H = K$.

6. Choose $x \in Ha \cap Hb$. Write $x = h_1 a = h_2 b$ for some $h_1, h_2 \in H$. Then $a = h_1^{-1} x$. Let $y \in Ha$. Then $y = ha$ for some $h \in H$ and so

$$y = ha = hh_1^{-1} x = hh_1^{-1} h_2 b \in Hb.$$

y being an arbitrary element of Ha, we conclude that $Ha \subset Hb$. A similar argument shows that $Hb \subset Ha$ as well, so that $Ha = Hb$.

7. Let G be a group of order 110. Let $x \in G$, $x \neq e$. Then $|x| \neq 1$ and divides $110 = 2 \cdot 5 \cdot 11$. It follows that $|x|$ must be divisible by one of the primes 2, 5 or 11. If this prime is p, then the cyclic subgroup $\langle x \rangle$ has a unique subgroup H of order p, which is also cyclic (by the Fundamental Theorem of Cyclic Groups). Since "being a subgroup of" is transitive, H is the cyclic subgroup of G we sought to prove existed.

8. Since $x^|G| = e$ for all $a \in G$, the exponent of a finite group must be finite (and $\leq |G|$). Let $n \in \mathbb{Z}^+$ be the exponent of G and suppose that m has the property that $x^m = e$ for all $x \in G$. Write $m = qn + r$ with $q \in \mathbb{Z}$ and $0 \leq r < n$. Then, for any $x \in G$ we have

$$x^r = x^{m-qn} = x^m (x^- q)^n = ee = e$$

which contradicts the choice of n as the least positive integer with this property unless $r = 0$. That is, if $x^m = e$ for all $x \in G$, then n divides m. Since $|G|$ has this property, we conclude that n divides $|G|$, i.e. the exponent of G divides $|G|$.

9. We know that the orders of elements in S_5 are given by the least common multiples of the terms in the possible partitions of 5 into positive integers. The partitions are

$$\begin{aligned}
5 &= 1+1+1+1+1 \\
5 &= 2+1+1+1 \\
5 &= 2+2+1 \\
5 &= 3+1+1 \\
5 &= 3+2 \\
5 &= 4+1 \\
5 &= 5
\end{aligned}$$

and the orders (lcm's) are $1, 2, 3, 4, 5, 6$. If $\sigma \in S_5$ then $\sigma^n = \epsilon$ if and only if n is a multiple of $|\sigma|$. Hence, if n is the exponent of S_5 then n is divisible by all of the orders of the elements of S_5. The least positive integer with this property is the least common multiple of $1, 2, 3, 4, 5, 6$ which is 60.

As above, the orders of the elements in S_6 are determined by the least common mutltiples of the terms in the possible partitions of 6 into positive integers. The partitions of 6 are

$$\begin{aligned}
6 &= 1+1+1+1+1+1 \\
6 &= 2+1+1+1+1 \\
6 &= 2+2+1+1 \\
6 &= 2+2+2 \\
6 &= 3+1+1+1 \\
6 &= 3+2+1 \\
6 &= 3+3 \\
6 &= 4+1+1 \\
6 &= 4+2 \\
6 &= 5+1 \\
6 &= 6
\end{aligned}$$

The question is, which of these partitions correspond to elements of A_6? Since an l-cycle can be written as a product of $l-1$ transpositions, a permutation with cycle structure corresponding to the partition $6 = l_1 + l_2 + \cdots l_k$ can be written as the product of $(l_1 - 1) + (l_2 - 1) + \cdots + (l_k - 1) = 6 - k$ transpositions. Hence, the permutations with cycle structure corresponding to the partition $6 = l_1 + l_2 + \cdots + l_k$ is even if and only if k is even. Therefore the orders of the elements of A_6 are given by the lcm's of the terms in the partitions of 6 into an even number of parts. These are easily identified in the list above, and their lcm's are 1, 2, 3, 4, 5. As above, it is the lcm of these orders that provide the exponent of A_6. Hence, the exponent of A_6 is also 60.

10. We will show that if p and q are distinct prime integers then $p(\mathbb{Q}^\times)^2 \neq q(\mathbb{Q}^\times)^2$. Since there are infinitely many primes in $\mathbb{Z}$, this will suffice to prove that there are infinitely many cosets of $(\mathbb{Q}^\times)^2$ in $\mathbb{Q}^\times$.

So, suppose that p, q are distinct prime integers. We know that $p(\mathbb{Q}^\times)^2 = q(\mathbb{Q}^\times)^2$ if and only if $p^{-1}q \in (\mathbb{Q}^\times)^2$ which happens if and only if there are non-zero integers a, b so that $p^{-1}q = (a/b)^2$, or $b^2q = a^2p$. However, this contradicts the fundamental theorem of arithmetic since q occurs an odd number of times in b^2q but an even number of times in a^2p (since $p \neq q$). We conclude that it is impossible to have $p(\mathbb{Q}^\times)^2 = q(\mathbb{Q}^\times)^2$ and hence that each prime integers gives rise to a distinct coset of $(\mathbb{Q}^\times)^2$ in $\mathbb{Q}^\times$, which is what we sought to show.

11. If $\phi : \mathbb{Q}^\times \to \mathbb{R}^\times$ is an isomorphism then $\phi(x)$ is a square if and only if x is a square. This is left as an exercise to the reader and is true of any group isomorphism. It follows from this that $\phi((\mathbb{Q}^\times)^2) = (R^\times)^2$. But then we'd have

$$\infty = [\mathbb{Q}^\times : (\mathbb{Q}^\times)^2] = [\phi(\mathbb{Q}^\times) : \phi((\mathbb{Q}^\times)^2)] = [\mathbb{R}^\times : (\mathbb{R}^\times)^2] = 2.$$

Here we have used the facts that isomorphisms preserve indices of corresponding subgroups and that $[\mathbb{R}^\times : (\mathbb{R}^\times)^2] = 2$, which was proven in class. The absurdity $\infty = 2$ shows that the existence of ϕ is impossible and so $\mathbb{Q}^\times \not\cong \mathbb{R}^\times$.

12. Since the cycles (13579) and (268) are disjoint, the order of β^2 is the lcm of their lengths, which is 15. Therefore

$$15 = |\beta^2| = \frac{|\beta|}{(|\beta|, 2)}.$$

Since $(|\beta|, 2) = 1$ or 2, we conclude that $|\beta| = 15$ or 30. It is not hard to see that 30 cannot be the order of an element of S_9 and so it must be that $|\beta| = 15$. But then $|\beta| = |\beta^2|$ so that $\langle\beta\rangle = \langle\beta^2\rangle$, which tells us that β is a power of β^2. Determining which power is easy enough: we need to find k so that $\beta^{2k} = \beta$ or, equivalently, $\beta^{2k-1} = \epsilon$. But this happens if and only if $15 = |\beta|$ divides $2k - 1$. $k = 8$ obviously satisfies this criterion. Therefore

$$\beta = \beta^{2\cdot 8} = \beta^{16} = (13579)^{16}(268)^{16} = (13579)^1(268)^1 = (13579)(268).$$

Here we have used the facts that (13579) and (268) commute and have orders 5 and 3, respectively.

13. We have seen that

$$\mathrm{Aut}(\mathbb{Z}_{25}) \cong U(25).$$

Moreover, it is straightforward to verify that $U(25)$ is cyclic of order 20, so that $U(25) \cong \mathbb{Z}_{20}$. Hence

$$\mathrm{Aut}(\mathrm{Aut}(\mathbb{Z}_{25})) \cong \mathrm{Aut}(U(25)) \cong \mathrm{Aut}(\mathbb{Z}_{20}) \cong U(20).$$