GROUPS AND RINGS, PROBLEM SHEET 3 SOLUTIONS

Question 1:

Conjugation preserves cycle shape in S_n, and any two elements of the same cycle shape are conjugate by some element of S_n. Indeed take two permutations of the same cycle shape in S^n. Write these elements in the same cycle order. For example consider (12)(345) and (13)(425). We can construct the element $g \in S_5$ which conjugates one to the other as follows. Consider the permutation defined by the following assignment:

$$\begin{array}{ccccc}(1 & 2) & (3 & 4 & 5) \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ (1 & 3) & (4 & 2 & 5)\end{array}$$

This is the permutation $g = (1)(234)(5)$. One can check that g conjugates the first element into the second. In general we can use this procedure to show any two cycles of the same shape are conjugate.

Thus cardinality of a given conjugacy class can be determined by counting the number of possible permutations of a fixed cycle shape.

Fix a given cycle shape. Let us count the number of possible elements x of that cycle shape. To initially assign the n numbers we have $n!$ possible choices.

For each i-cycle in x, we must divide by i since (for example) (1234) is the same group element as (2341) and we have in general i ways of rearranging this i-cycle. Let m_i be the number of i-cycles in x. Since disjoint cycles commute, we also can rearrange our m_i i-cycles freely and there are $m_i!$ ways of doing this, so we must also divide out by $m_i!$. Thus we obtain

$$\frac{n!}{\prod_{i=1}^{n} i^{m_i} m_i!}$$

possible choices of element x of our given cycle shape.

Question 2:

Notice that $|V| = 4$ and $|S_4| = 24$. Thus if we could find a homorphism from S_4 to a group of order 6, we could hope that V is the kernel of this homomorphism. Since $|S_3| = 6$, let's look for a homomorphism $S_4 \to S_3$.

Let x_1, x_2, x_3, x_4 be four variables and define three polynomials by

$$p_1 = x_1x_2 + x_3x_4, \quad p_2 = x_1x_3 + x_2x_4, \quad p_3 = x_1x_4 + x_2x_3.$$

A permutation of $\{x_1, x_2, x_3, x_4\}$ induces a permutation of the polynomials $\{p_1, p_2, p_3\}$ and thus we obtain a homomorphism

$$f : S_4 \to S_3.$$

A permutation fixes each of p_1, p_2, p_3 if and only if it is the identity or a product of two 2-cycles. That is, $V = \ker f$. Since V is the kernel of a group homomorphism, it is a normal subgroup of S_4. Since every non-identity element of V has order two, it cannot be isomorphic to C_4, so $V \cong C_2 \times C_2$.

(Note that for $n \geq 5$, the only normal subgroup of S_n is A_n, so the case $n = 4$ with $V \lhd S_4$ is quite exceptional.)

Every element of S_4 acts trivially by conjugation on $e \in V$, so $S_4 \cdot e = e$ and $(S_4)_e = S_4$. There is one other orbit consisting of the remaining three elements of V. Indeed notice that conjugating (12)(34) by (1234) gives (14)(23) and by (123) gives (13)(24). By the orbit-stabiliser theorem the stabiliser of any of these elements must be order $24/3 = 8$. The only subgroups of order 8 in S_4 are D_8 and its two conjugacy subgroups.

Explicitly, take (for example) the stabiliser $H < S_4$ of (12)(34). Then since V itself is Abelian, (12)(34) is fixed by conjugation of any element of V, so $V < H$ giving us four elements. Also (12) and (34) clearly fix (12)(34). Since our stabiliser should be a closed subgroup, we must also add in $(13)(24)(12) = (1423)$ and $(14)(23)(12) = (1324)$ which completes our subgroup isomorphic to D_8.

Question 3:

Taking a quotient G/H "shrinks the subgroup H to zero inside G," so intuitively if G_{tors} is the subgroup of all torsion elements, we expect that G/G_{tors} will have no (non-identity) torsion elements.

Explicitly, if $g + G_{\text{tors}}$ is torsion in G/G_{tors}, then $n(g + G_{\text{tors}}) = ng + G_{\text{tors}} = G_{\text{tors}}$. Thus $ng \in G_{\text{tors}}$. But then there exists an m such that $mng = 0$, so $(mn)g = 0$ and $g \in G_{\text{tors}}$ so $g + G_{\text{tors}} = 0$ in G/G_{tors}.

Question 4:

The easiest way to show two groups are not isomorphic is to compare their cardinalities, but $\mathbb{Z}^n$ and $\mathbb{Z}^m$ have the same cardinality (countably infinite). Intuitively if $n > m$ then $\mathbb{Z}^n$ should have "more" elements than $\mathbb{Z}^m$.

Let us reduce to a statement about finite groups. Suppose $\mathbb{Z}^n \cong \mathbb{Z}^m$. Then $\mathbb{Z}^n/2\mathbb{Z}^n \cong \mathbb{Z}^m/2\mathbb{Z}^m$. But $\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdot \times \mathbb{Z}}_{n \text{ times}}$ and in problem sheet 1 we saw that the quotient of a product group by a product subgroup is the product of the quotients. Thus $\mathbb{Z}^n/2\mathbb{Z}^n \cong (\mathbb{Z}/2\mathbb{Z})^n$. This has 2^n elements. On the other hand $\mathbb{Z}^m/2\mathbb{Z}^m$ has 2^m elements, so we can only have $\mathbb{Z}^n \cong \mathbb{Z}^m$ if $n = m$.

Question 5:

Intuition: a matrix A scales the unit parallelopiped in $\mathbb{R}^n$ into a new parallelopiped of volume $\det A$. If one restricts to the lattice $\mathbb{Z}^n$, then one expects that any elements contained inside this new parallelopiped of volume $\det A$ will be missed by $A\mathbb{Z}^n$ and will be non-zero in the quotient group $\mathbb{Z}^n/A\mathbb{Z}^n$. There should be approximately $\det A$ of these elements, so we expect the quotient group to have size $|\det A|$.

Using Smith normal form we can reduce the problem to considering just a diagonal matrix, which scales each coordinate separately. If $Q \in \mathrm{GL}(n, \mathbb{Z})$ is an invertible matrix, then $Q\mathbb{Z}^n = \mathbb{Z}^n$, so $AQ\mathbb{Z}^n = A\mathbb{Z}^n$. On the other hand if $P \in \mathrm{GL}(n, \mathbb{Z})$ then the automorphism $\varphi : x \mapsto Px$ of $\mathbb{Z}^n$ maps $A\mathbb{Z}^n$ isomorphically onto $PA\mathbb{Z}^n$. Thus

$$\mathbb{Z}^n/A\mathbb{Z}^n \cong P\mathbb{Z}^n/PA\mathbb{Z}^n = \mathbb{Z}^n/PA\mathbb{Z}^n = \mathbb{Z}^n/PAQ\mathbb{Z}^n.$$

Since any A can be brought into diagonal form $\mathrm{diag}(a_1, \ldots, a_n) = PAQ$ over the integers by invertible matrices P and Q, we have reduced to the case of diagonal matrices.

In this case again we see that $A\mathbb{Z}^n$ is a product of subgroups $a_i\mathbb{Z} < \mathbb{Z}$ for each i, and so

$$\mathbb{Z}^n/A\mathbb{Z}^n \cong \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}$$

which has order $|a_1 \cdots a_n| = \det A$.

Question 6:

Consider our element $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. Let us write the subgroup H generated by this element in the form $h\mathbb{Z}^n$ for some matrix h. Then similarly to the previous question we can apply the Smith normal form to reduce to a simpler situation.

Let us take the matrix h as

$$h = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix}.$$

Note that we could have taken the numbers $a_1, \ldots, a_n$ to lie in any column. Then $h\mathbb{Z}^n = H$.

This matrix has Smith normal form

$$h' = \begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

where $d = \gcd(a_1, \ldots, a_n)$.

We have now reduced to the case of taking a quotient of $\mathbb{Z}^n$ by the subgroup generated by the element $(d, 0, \ldots, 0)$. This is the subgroup $d\mathbb{Z} \times 0 \times \cdots \times 0$. By problem sheet 1 we know that the quotient by a product subgroup is the product of the quotients, so we have

$$\mathbb{Z}^n/H \cong \mathbb{Z}^n/h\mathbb{Z}^n \cong \mathbb{Z}^n/h'\mathbb{Z}^n \cong (\mathbb{Z}/d\mathbb{Z}) \times \mathbb{Z}^{n-1}.$$

Now we see that the rank of $\mathbb{Z}^n/H$ is $n-1$ and the torsion subgroup is $\mathbb{Z}/d\mathbb{Z}$.

Question 7:

Since every subgroup of a cyclic group is cyclic, if G contains a subgroup isomorphic to $C_p \times C_p$ then G cannot be cyclic (since $C_p \times C_p$ isn't because $\gcd(p,p) = p \neq 1$).

Now suppose G is not cyclic. Since G is a finite Abelian group, it is isomorphic to a direct product of cyclics groups of prime power order. Furthermore, since a product of cyclic groups of order a, b with $\gcd(a,b) = 1$ is itself cyclic, we must have that there are two factors $C_{p^{k_1}} \times C_{p^{k_2}}$ which are powers of the *same* prime p. Then this product of cyclic groups contains a copy of $C_p \times C_p$.

Question 8:

If $S \subset G$ is finite and closed under group multiplication, then every element of S has finite order and every power of it is contained in S. Let $a \in S$ with order m. Then $a^m = e$ so $a^{m-1} = a^{-1}$. Thus S is also closed under taking inverses so it is a subgroup.

This fails for infinite sets where elements can have infinite order. For example $\mathbb{N} \subset \mathbb{Z}$ is closed under addition but not taking inverses.

(Secretly what is being used here is that an injective function between finite sets of the same size is always surjective and hence a bijection, this fact is not true for infinite sets! Later you may use this same trick to prove that every finite integral domain is a field.)