EXERCISE SHEET 1 WITH SOLUTIONS

(E8) Prove that, given a transitive action of G on Ω, there exists a subgroup $H \leq G$ such that the action of G on Ω is isomorphic to the action of G on $H\backslash G$. You may need to recall what it means for two group actions to be isomorphic.

> **Answer.** Let $\omega \in \Omega$ and set $H := G_\omega$. Define
> $$f : \Omega \to H\backslash G, \omega_1 \mapsto Hg_1$$
> where $\omega^{g_1} = \omega_1$. It is clear that f is well-defined and bijective. Now observe that, for $\omega_1 \in \Omega$ and $g \in G$,
> $$f(\omega_1^g) = f(\omega^{g_1 g}) = Hg_1 g = (Hg_1)g = (f(\omega_1))^g.$$
> The result follows.

(E12) Let G be a finite group acting transitively on a set Ω. Show that the average number of fixed points of the elements of G is 1, i.e.

$$\frac{1}{|G|}\sum_{g\in G} |\{\omega \in \Omega \mid \omega^g = \omega\}| = 1.$$

> **Answer.** Consider the set
> $$\Lambda := \{(\omega, g) \in \Omega \times G \mid \omega^g = g\}.$$
> We count $|\Lambda|$ in two different ways. Observe that there are $|\Omega|$ possibilities for the first entry, and for each such entry there are $|G_\omega|$ possibilities for the second entry. On the other hand there are $|G|$ possibilities for the second entry and, for each such entry there are d possibilities for the first entry. (Here we write d for the average number of fixed points of elements in G.) We conclude that
> $$|\Omega| \cdot |G_\omega| = |G| \cdot d.$$
> Now the orbit-stabilizer theorem yields the result.

(E14) For which values of n is the action of D_{2n} on an n-gon, 2-transitive?

> **Answer.** In order to be 2-transitive, D_{2n} must be transitive on pairs of distinct vertices, a set of size $n(n-1)$. Thus a necessary condition for 2-transitivity is that $n(n-1)$ divides $|D_{2n}| = 2n$. We conclude that the only possible value for n is 3. It is easy to verify that when $n = 3$, the action is, indeed 2-transitive. (Indeed it is 3-transitive!)

(E19) Prove that G acts primitively on Ω if and only if G acts transitively and any stabilizer, G_ω, is a maximal subgroup of G.

Answer. That primitivity implies transitivity is obvious, since orbits are G-congruences.

Now suppose that $\sim$ is a non-trivial G-congruence and let Λ be a block of imprimitivity for $\sim$ containing a point ω. Now define

$$G_\Lambda := \{g \in G \mid \lambda^g \in \Lambda \text{ for all } g \in G\}.$$

Clearly G_Λ is a group and it contains G_ω.

Note first that if $G_\Lambda = G$, then $\Lambda = \Omega$ which contradicts the fact that $\sim$ is non-trivial. On the other hand, since $\sim$ is non-trivial there exists $\omega_1 \in \Lambda \backslash \{\omega\}$ and, since G is transitive, there exists $g \in G$ such that $\omega^g = \omega_1$. Since G_Λ contains g we conclude that G_ω is a proper subgroup of G_Λ as required.

On the other hand suppose that $G_\omega < H < G$ for some subgroup H. We must show that G acts imprimitively. We define an equivalence relation $\sim$ on Ω as follows:

$$\alpha \sim \beta \iff G_\alpha, G_\beta < H^g, \exists g \in G.$$

It is easy to see that $\sim$ is well-defined; we must show it is non-trivial. If there is one equivalence class, then H is transitive and contains G_Ω, hence $H = G$, a contradiction. If all equivalence classes are singletons, then no element of H moves ω and so $G_\omega = H$, a contradiction. We are done.

(E21) Use Iwasawa's criterion to show that A_n is simple for $n \geq 5$. Hint: consider the action on unordered triples from $\{1, \ldots, n\}$.

Answer. *I'll just prove the result for $n \geq 7$. The other cases can be done directly.*

Let Λ be the set of all unordered triples from $\{1, \ldots, n\}$, and consider the natural action of $G = A_n$ on Λ given by

$$\{\lambda_1, \lambda_2, \lambda_3\}^g := \{\lambda_1^g, \lambda_2^g, \lambda_3^g\}.$$

It is easy to see that this action is faithful.

It is easy to see that the stabilizer of a point λ in Λ is isomorphic to $(S_3 \times S_{n-3}) \cap A_n$.

Claim: The 3-cycles generate A_n if $n \geq 4$.

Proof of claim: Any element of A_n can be written as a product of an even number of transpositions. We claim that any pair of transpositions in such a product can be replaced by one or two 3-cycles. There are two cases.

– The transpositions move distinct points. But then we use the fact that

$$(1,2,3)(1,2,4) = (1,3)(2,4).$$

– The transpositions have one point in common. But then we use the fact

$$(1,2,3) = (1,2)(2,3).$$

Claim: If $n \geq 7$, then the stabilizer of a point in Λ is maximal in A_n. In particular G acts on Λ primitively.

Proof of claim: Let H be the stabilizer of $\{1,2,3\} \in \Lambda$ and notice that H has orbits $\{1,2,3\}$ and $\{4, \ldots, n\}$ in the action on $\{1, \ldots, n\}$. Any elements that normalizes H must either fix these orbits, of permute them. But since they are of different sizes, we conclude that an element must fix the orbits, and hence lies in H, i.e. $N_G(H) = H$.

Let $H < M \leq G$. Since $N_G(H) = H$ we conclude that M contains a distinct conjugate of H. This conjugate must contain a 3-cycle containing at least one element from $\{1, 2, 3\}$ and at least one element from $\{4, \dots, n\}$. Without loss of generality, we may assume that the 3-cycle is $(1, 2, 4)$ or $(1, 4, 5)$.

In the former case it is easy to see that M contains $\mathrm{Alt}(\{1, 2, 3, 4\})$, the alternating group on $\{1, 2, 3, 4\}$. With slightly more work one can see, in the second case that M contains $\mathrm{Alt}(\{1, 2, 3, 4, 5\})$. Now we induct. Suppose that M contains $\mathrm{Alt}(\{1, \dots, k\})$. It is obvious that the stabilizer in M of $\{1, \dots, k+1\}$ is transitive on $\{1, \dots, k+1\}$, and so M contains $\mathrm{Alt}(\{1, \dots, k+1\})$. We conclude that $M = G$ as required.

Claim: The stabilizer of $\{1, 2, 3\}$ has a normal abelian subgroup whose normal closure is G.

Proof of Claim: The subgroup $\langle(1, 2, 3)\rangle$ is obviously normal and abelian. Its normal closure is G by virtue of the fact that it contains a 3-cycle, that all 3-cycles are conjugate, and that the 3-cycles generate G.

Claim: A_n is perfect for $n \geq 5$.

Proof of Claim: We need only show that G' contains a 3-cycle. But this follows from

$$(2, 5, 1)(3, 2, 4)(1, 5, 2)(4, 2, 3) = (2, 5, 4).$$

Now the result follows by Iwasawa's Criterion.

(E22) Prove the following variant on Iwasawa's criterion: Suppose that G is a finite perfect group acting faithfully and primitively on a set Ω, and suppose that the stabilizer of a point has a normal soluble subgroup S, whose conjugates generate G. Then G is simple.

Answer. Let K be a normal non-trivial subgroup of G. Lemma 2 of lectures implies, therefore, that K acts transitively on Ω and hence $G = G_\omega K$. Thus, for all $g \in G$, there exists $g_1 \in G_\omega, k \in K$ such that $g = g_1 k$ and this implies, in particular, that

$$\{S^g \mid g \in G\} = \{S^k \mid k \in K\}.$$

Now, since $\langle S^k \mid k \in K\rangle \leq SK \leq G$ we conclude that $G = SK$. Then

$$G/K = SK/K \cong S/S \cap K.$$

Since the right hand side is a quotient of a solvable group it must itself be solvable, and we conclude that G/K is solvable. Since the derived series of a solvable group terminates at $\{1\}$ we conclude that either G/K is trivial (and we are done) or G/K is not perfect, i.e. G/K has an abelian quotient. But the latter implies that G has an abelian quotient which contradicts the fact that G is perfect.

(E23) Check that the definition of a semi-direct product given in lectures gives a well-defined group. If ϕ is the trivial homomorphism, what is $K \rtimes_\phi H$?

Answer. Group multiplication was given by

$$(h_1, k_1)(h_2, k_2) = (h_1 \cdot h_2, k_1^{\phi(h_2)} \cdot k_2).$$

Closure is clear. I will leave associativity for the bracket fanatic. Observe that $(1, 1)$ is an identity element and that the inverse of (h_1, k_1) is given by $(h_1^{-1}, (k_1^{\phi(h_1^{-1})})^{-1})$.

(E24) Prove Lemma 4 from lectures.

Answer. This is Theorem 9.9 of Rose's *A course on group theory*. Or can be found in any standard book on group theory.

(E29) Show that Vandermonde's Theorem does not hold in the octonions, $\mathbb{H}$.

Answer. Take $f(X) = X^2 + 1$. Then i, j and k are all roots of f.

(E30) Show that $X^2+1 \in \mathbb{F}_3[X]$ is irreducible, and compute the addition and multiplication tables for $\mathbb{F}_9 := \mathbb{F}_3[x]/\langle X^2 + 1\rangle$.

Answer. If $X^2 + 1$ were reducible it would have a root, but it doesn't. An addition table is hardly necessary as one just does normal polynomial addition. Multiplication is the interesting one. I write $a + b\alpha$ for $a + bX + \langle X^2 + 1\rangle$ in $\mathbb{F}_3[x]/\langle X^2 + 1\rangle$.

	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+1$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	2	$\alpha+2$	$2\alpha+2$	1	$\alpha+1$	$2\alpha+1$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$\alpha+2$	2α	1	$2\alpha+1$	2	α
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	1	α	$\alpha+1$	2α	2
2α	0	2α	α	1	$2\alpha+1$	$\alpha+1$	2	$2\alpha+2$	$\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$\alpha+1$	2	2α	$2\alpha+2$	α	1
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$2\alpha+1$	α	2	$\alpha+2$	1	2α

(E31) Show that $X^3 + X + 1 \in \mathbb{F}_2[X]$ is irreducible, and compute the addition and multiplication tables for $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle X^3 + X + 1\rangle$.

Answer. Same method as the previous. I'll do this on request (I'm losing the will to live).

(E32) Fix a basis B of V. Prove that any semilinear transformation on V is a composition of a linear transformation and a field automorphism of V with respect to B.

Answer. Define $T_0 := \alpha^{-1}T$ where α is the associated automorphism of T. It is sufficient to prove that T_0 is linear. It is clearly additive. What is more if $c \in k$ and $v \in V$, then

$$(cv)T_0 = (c^{\alpha^{-1}} v^{\alpha^{-1}})T = (c^{\alpha^{-1}})^{\alpha}(v^{\alpha^{-1}})T) = cvT_0.$$

We are done.

(E33) Prove that $\Gamma\mathrm{L}_n(k) \cong \mathrm{GL}_n(k) \rtimes_\phi \mathrm{Aut}(k)$. You will need to choose an appropriate homomorphism $\phi : \mathrm{Aut}(k) \to \mathrm{Aut}(\mathrm{GL}_n(K))$ to make this work. You may find it convenient to fix a basis for V – so you can express elements of $\mathrm{GL}_n(k)$ as matrices – before you choose ϕ.

Answer. Observe that H, the set of field automorphisms of V is a subgroup of $\Gamma\mathrm{L}_n(k)$ isomorphic to $\mathrm{Aut}(k)$.

Claim: $H \cap \mathrm{GL}_n(k) = \{1\}$

Proof of claim: Observe that H fixes all of the vectors whose entries are either 1 or 0. The only elements of $\mathrm{GL}_n(k)$ that do this are scalar multiples of 1. Now consider a vector $v = (\alpha, 1, \dots, 1)$. Any element of H that moves α will map v to a vector that is not scalar multiple of v. Since every non-trivial element of H moves some non-zero element of k, the claim follows.

This claim, and (E32), implies that every element of G has a unique representation as αT where $T \in \mathrm{GL}_n(k)$ and $\alpha \in \mathrm{Aut}(k)$.

Claim: $\mathrm{GL}_n(k)$ is a normal subgroup of $\Gamma\mathrm{L}_n(k)$.

Proof of claim: Let $T \in \mathrm{GL}_n(k)$ and let α be a field automorphism of V. Let $c \in k, v \in V$ and observe that

$$(cv)\alpha^{-1}T\alpha = (c^{\alpha^{-1}} v^{\alpha^{-1}})T\alpha = ((c^{\alpha^{-1}})(v^{\alpha^{-1}}T))\alpha = c(v^{\alpha^{-1}}T\alpha).$$

Thus $\alpha^{-1}T\alpha$ is linear and the claim follows.

This claim yields an automorphism $H \to \mathrm{Aut}(\mathrm{GL}_n(k))$ given by the conjugation action of H on $\mathrm{GL}_n(k)$. Now given two elements $g_1, g_2 \in \Gamma\mathrm{L}_n(k)$ we can write them as $T_1\alpha_1$ and $T_2\alpha_2$ and obtain that

$$(\alpha_1 T_1)(\alpha_2 T_2) = (\alpha_1\alpha_2)(\alpha_2^{-1}T_1\alpha_2 T_2) = \alpha_1\alpha_2 T_1^{\phi(\alpha_2)} T_2$$

and we are done.