

# Exercises on chapter 1

1. Let  $G$  be a group and  $H$  and  $K$  be subgroups. Let  $HK = \{hk \mid h \in H, k \in K\}$ .
  - (i) Prove that  $HK$  is a subgroup of  $G$  if and only if  $HK = KH$ .
  - (ii) If either  $H$  or  $K$  is a normal subgroup of  $G$  prove that  $HK$  is a subgroup of  $G$ . If both  $H$  and  $K$  are normal subgroups of  $G$ , prove that  $HK$  is a normal subgroup of  $G$ .
  - (iii) Prove that  $[H : H \cap K] \leq [G : K]$ . (Note this makes sense even for infinite groups if we define the index  $[G : K]$  to be the number of left cosets of  $K$  in  $G$ , or  $\infty$  if there are infinitely many). Moreover, if  $[G : K]$  is finite, then  $[H : H \cap K] = [G : K]$  if and only if  $G = HK$ .
  - (iv) If  $H, K$  are of finite index such that  $[G : H]$  and  $[G : K]$  are relatively prime, then  $G = HK$ .
    - (i) If  $HK$  is a subgroup of  $G$  then its closed under inverses so  $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$ . Conversely if  $HK = KH$  then take  $hk, h'k' \in HK$ . Then  $(hk)(h'k')^{-1} = hk(k')^{-1}(h')^{-1}$ . Since  $HK = KH$  we can rewrite  $k(k')^{-1}(h')^{-1}$  as  $h''k''$  for some new  $h'' \in H, k'' \in K$ . So its  $hh''k''$  which is in  $HK$ . This verifies that  $HK$  is a subgroup.
    - (ii) If  $H$  is normal in  $G$  then we get that  $Hk = kk^{-1}Hk = kH$  for every  $k \in K$ . Hence  $HK = KH$  so its a subgroup by (i). If they're both normal in  $G$  its obvious that  $HK$  is too.
    - (iii) The map  $H/(H \cap K) \rightarrow G/K, h(H \cap K) \mapsto hK$  is a well-defined injection. Now consider  $HK/K$  as an orbit of the group  $H$ . The point stabilizer of  $1K$  is  $H \cap K$ . Hence  $[HK : K] = [H : H \cap K]$ . So we deduce that  $[H : H \cap K] = [G : K]$  if and only if  $[HK : K] = [G : K]$ , which is clearly if and only if  $G = HK$ .
    - (iv) By (iii),  $G = HK$  if and only if  $[H : H \cap K] \geq [G : K]$ , which is if and only if  $[G : H \cap K] \geq [G : K][G : H]$ . Note that  $[G : H \cap K] = [G : H][H : H \cap K]$  and  $[G : H \cap K] = [G : K][K : H \cap K]$ . So both  $[G : H]$  and  $[G : K]$  already divide  $[G : H \cap K]$ , whence since they're relatively prime  $[G : H][G : K]$  divides  $[G : H \cap K]$ . We're done.
2. Recall that a partially ordered set  $X$  is called a *complete lattice* if every non-empty subset of  $X$  has both a least upper bound and a greatest lower bound in  $X$ . Prove that the set of all normal subgroups of a group  $G$  partially ordered by inclusion forms a complete lattice.
 

Recall how the poset of *all* subgroups is a complete lattice: the greatest lower bound is the intersection and the least upper bound is the subgroup generated by the given subgroups. So to show that normal subgroups form a complete lattice too we just need to observe that the intersection of normal subgroups is normal, and the subgroup generated by a bunch of normal subgroups is normal. Let me just to the last thing, since everything else is clear.

So take normal subgroups  $(K_i)_{i \in I}$ . The subgroup generated by them is the intersection  $N$  of all subgroups of  $G$  containing all  $K_i$ . The conjugate of  $N$  by  $g \in G$  is also a subgroup of  $G$  containing all  $K_i$ . Hence  $N = {}^gN$ .
3. Let  $N$  be a normal subgroup of index 2 in a finite group  $G$ . For example,  $N = A_n, G = S_n$  for  $n \geq 2$ .
  - (i) Let  $X$  be a  $G$ -set and  $x \in X$ . Prove that  $G \cdot x = N \cdot x$  if  $G_x \not\leq N$ ; otherwise the  $G$ -orbit  $G \cdot x$  splits into two  $N$ -orbits of the same size.

(ii) Compute the number of conjugacy classes in the alternating group  $A_6$  together with their orders.

(i) Recall that  $|G \cdot x| = [G : G_x]$ . If  $G_x \leq N$  then  $N_x = N \cap G_x = G_x$ . So  $|N \cdot x| = |N|/|G_x| = |G \cdot x|/2$ . So in this case the  $G$ -orbit of  $x$  splits into two  $N$ -orbits each of half the size.

Otherwise,  $N_x$  is strictly smaller size than  $G_x$ . Since  $[G_x : N_x] = [G_x : N \cap G_x] = [G_x + N : N]$  and  $N$  is of index 2 in  $G$ , it follows that  $[G_x : N_x] = 2$  exactly. Hence,  $|N \cdot x| = [N : N_x] = [G : G_x] = |G \cdot x|$  and the  $G$ -orbit equals the  $N$ -orbit.

(ii) The cycle shapes of even permutations in  $S_6$  are as follows:  $(5, 1), (4, 2), (3, 1, 1, 1), (3, 3), (2, 2, 1, 1, 1), (1, 1, 1, 1, 1, 1)$ . The sizes of the corresponding conjugacy classes are as follows: 144, 90, 40, 40, 45, 1. We just need to determine which of these split into two conjugacy classes in  $A_6$ : a conjugacy class splits if the centralizer of such an element consists just of even permutations. For example for  $(5, 1)$ , the centralizer consists is the subgroup generated by the 5-cycle, so its just even stuff, so it splits. On the other hand for  $(4, 2)$ , the centralizer contains the transposition part which is odd, so it doesn't split. You deduce: splits, doesn't split, doesn't split, doesn't split, doesn't split, doesn't split. So there are 7 conjugacy classes of sizes 72, 72, 90, 40, 40, 45, 1.

4. Prove that any infinite group has infinitely many subgroups. If the group contains an element of infinite order, then it contains a copy of  $\mathbb{Z}$ , which has infinitely many subgroups  $(2\mathbb{Z}, 3\mathbb{Z}, \dots)$ . So we may assume every element is of finite order. Take  $g_1 \in G$ . Then we have the cyclic subgroup  $\langle g_1 \rangle$  which is finite. So we can pick  $g_2 \in G - \langle g_1 \rangle$ . This gives another subgroup  $\langle g_2 \rangle$ . Then pick  $g_3 \in G - (\langle g_1 \rangle \cup \langle g_2 \rangle)$ . Continue...

5. Compute the group  $\text{Aut}(C_8)$  of automorphisms of the cyclic group  $C_8$  of order 8. Is it cyclic?

It is easiest to think of  $C_8$  additively as  $\mathbb{Z}_8$  and compute  $\text{Aut}(\mathbb{Z}_8)$  instead. Then that is just the group  $\mathbb{Z}_8^\times$  of units in the ring  $\mathbb{Z}_8$ . The units are 1, 3, 5, 7. This multiplicative group is isomorphic to  $V_4$ , the Klein 4-group: all of these elements are of order 2. No its not cyclic as there is no element of order 4.

6. Let  $G$  be a finite group,  $H \trianglelefteq G$  and  $N \trianglelefteq H$ .

(i) Give a counterexample to show that it is not necessarily the case that  $N \trianglelefteq G$ .

(ii) If  $(|N|, [H : N]) = 1$ , prove that  $N$  is the unique subgroup of  $H$  having order  $|N|$ . Deduce that  $N \trianglelefteq G$ .

(iii) Show that  $A_4$  has a unique subgroup of order 4 and that this is a normal subgroup of  $S_4$ .

(i) Well the first thing I cooked up was to take the Klein 4-group  $C_2 \times C_2$  and make  $C_2$  act on it by sending  $(x, y)$  to  $(y, x)$ . Then form the semidirect product  $(C_2 \times C_2) \rtimes C_2$ , so  $C_2 \times C_2$  is normal in this of index 2. Consider then  $C_2 \times 1$  which is normal in  $C_2 \times C_2$ . It is not normal in the full semidirect product since the outside  $C_2$  sends  $C_2 \times 1$  to  $1 \times C_2$ .

This is better known as the dihedral group  $D_4$  with reflection  $h$  and rotation  $g$ . The subgroup  $C_2 \times C_2$  is generated by the reflections  $h$  and  $g^2h$ . The subgroup  $C_2 \times 1$  is just the subgroup generated by  $h$  itself. But its not normal in the whole group since  $ghg^{-1} = g^2h$ .

(ii) If  $K \leq H$  is another subgroup with  $|K| = |N|$ , then elements of  $K$  have orders prime to  $[H : N]$ , so  $kN$  must be 1 in  $H/N$  for any  $k \in K$ . This proves that  $K \subseteq N$ . Hence if we take any  $g \in G$  and conjugate, we get that  ${}^gN$  is a subgroup of  ${}^gN = N$  of the same order as  $N$ , hence it equals  $N$ . Hence  $N \trianglelefteq G$ .

(iii)  $A_4$  is normal in  $S_4$  of index 3. So its the unique subgroup of  $S_4$  of order 4 and its normal in  $S_4$  by (ii). (All obvious anyway but it illustrates the problem...)

7. A group  $G$  is called *metabelian* if there exists a normal subgroup  $N$  of  $G$  with  $N$  and  $G/N$  both abelian. Prove that every subgroup and every quotient of a metabelian group is metabelian.

Let  $H \leq G$ . Then the normal subgroup  $H \cap N$  of  $H$  is abelian, and the quotient group  $H/(H \cap N) \cong HN/N$  is abelian since its a subgroup of  $G/N$ .

Let  $K \trianglelefteq G$ . The group  $G/K$  has a normal subgroup  $KN/K \cong N/N \cap K$  so its abelian as its a quotient of  $N$ , and  $(G/K)/(KN/K) \cong G/KN$  so its abelian as its a quotient of  $G/N$ .

8. This is a question about the dihedral group  $D_n$  of order  $2n$ . Recall this is the subgroup of  $O(2)$  generated by two elements,  $g$  of order  $n$  (counterclockwise rotation through angle  $2\pi/n$ ) and  $h$  (reflection in the  $x$ -axis) of order 2, subject to the one relation that  $hg = g^{-1}h$ .

(i) For which  $n$  is the center  $Z(D_n)$  trivial?

(ii) For which  $n$  do the involutions (= elements of order 2) in  $D_n$  form a single conjugacy class?

(iii) Prove that the subgroup of all upper unitriangular  $3 \times 3$  matrices with entries in the field  $\mathbb{F}_2$  of two elements is isomorphic to  $D_4$ .

(iv) Is  $D_6 \cong S_3 \times C_2$ ?

(i) Let me do rather more, and work out the conjugacy classes in  $D_n$ . Remember the elements are  $1, g, \dots, g^{n-1}$  and  $h, hg, \dots, hg^{n-1}$ . We have that  $g$  is conjugate to  $g^{n-1}$ ,  $g^2$  is conjugate to  $g^{n-2}, \dots$ ;  $h$  is conjugate to  $hg^2, hg^4, \dots$  and  $hg$  is conjugate to  $hg^3, hg^5, \dots$ .

So if  $n$  is even then the conjugacy classes are  $\{1\}, \{g, g^{n-1}\}, \dots, \{g^{n/2-1}, g^{n/2+1}\}, \{g^{n/2}\}$  together with  $\{h, hg^2, \dots, hg^{n-2}\}$  and  $\{hg, hg^3, \dots, hg^{n-1}\}$ .

If  $n$  is odd then the conjugacy classes are  $\{1\}, \{g, g^{n-1}\}, \dots, \{g^{(n-1)/2}, g^{(n+1)/2}\}$  together with  $\{h, hg, \dots, hg^{n-1}\}$ .

Now the center is the conjugacy classes with just one element. So its trivial if and only if  $n$  is odd.

(ii) All  $hg^i$  are involutions. So if involutions form a single conjugacy class we must have that  $n$  is odd. In that case no  $g^i$  is an involution. So the answer is *if and only if  $n$  is odd*.

(iii) Map the canonical generators  $g$  and  $h$  of  $D_4$  to the matrices

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

respectively.

(iv) Yes. Think of  $D_6$  as symmetries of the regular hexagon. Then the symmetries which preserve the obvious equilateral triangle spanned by alternate vertices gives a subgroup isomorphic to  $S_3$  (generated by  $g^2$  and  $x$  say), and the rotation through 180 degrees gives a subgroup isomorphic to  $C_2$  (generated by  $g^3$ ). These two subgroups are normal, have trivial intersection and their product is everything.

9. (i) Suppose that  $G$  is an abelian group and  $g, h \in G$  are elements of orders  $n = |g|$  and  $k = |h|$  respectively. If  $n$  and  $k$  are relatively prime, i.e. their greatest common divisor  $(n, k)$  is 1, show that  $|gh| = nk$ .

(ii) Let  $G$  be a finite group of order  $n$ . If  $G$  is cyclic prove that  $G$  has a unique subgroup of order  $d$  for each divisor  $d$  of  $n$ , and moreover this subgroup is cyclic. Conversely, if  $G$  has at most one cyclic subgroup of order  $d$  for each divisor  $d$  of  $n$ , prove that  $G$  is cyclic.

(iii) Explain why the equation  $x^n = 1$  has at most  $n$  solutions in a field  $K$ .

(iv) Now let  $G$  be a finite subgroup of the group  $K^\times$  of units of some field  $K$ . Prove that  $G$  is cyclic.

(i) Let  $d = |gh|$ . Note since  $G$  is abelian that  $(gh)^{nk} = g^{nk}h^{nk} = 1$ . So  $d|nk$ .

Now write  $1 = an + bk$ . Then  $d = dan + dbk$ . So  $1 = (gh)^{dan} = g^{dan}h^{dan} = h^{d-dbk} = h^d$ . So  $k|d$ . Similarly,  $n|d$ . Hence  $LCM(n, k) = nk|d$ .

Hence  $d = nk$ .

(ii) Suppose that  $G$  is cyclic, say  $G = \langle x \rangle$  with  $x^n = 1$ . If  $d|n$  then  $x^{n/d}$  generates a cyclic subgroup of  $G$  of order  $d$ . Now we just need to show  $G$  has a unique subgroup of order  $d$ . Every subgroup

of a cyclic group is cyclic (because  $\mathbb{Z}$  is a PID) so we may assume that our cyclic subgroup is  $\langle y \rangle$  for some  $y \in G$  of order  $d$ . But then  $y = x^m$  for some  $m$  and  $y^d = 1$ , hence  $x^{md} = 1$ , hence  $n|md$ . Hence  $y = (x^{n/d})^{md/n}$ . This shows that  $y \in \langle x^{n/d} \rangle$ . Hence  $\langle y \rangle = \langle x^{n/d} \rangle$  and our subgroup is unique.

To prove the converse, some recollections. First, Euler's  $\phi$  function is defined by letting  $\phi(n)$  equal the number of units in the ring  $\mathbb{Z}_n$ . From this definition and the Chinese Remainder Theorem it follows that  $\phi(n_1 \dots n_s) = \phi(n_1) \dots \phi(n_s)$  if  $n_1, \dots, n_s$  are relatively prime integers. This means you can compute  $\phi(n)$  if you know how to compute  $\phi(p^r)$  for a prime  $p$ :  $\phi(p^r) = p^r - p^{r-1}$ .

Equivalently,  $\phi(n)$  is the number of  $1 \leq m < n$  with  $(m, n) = 1$ . Equivalently,  $\phi(n)$  is the number of primitive  $n$ th roots of 1 in  $\mathbb{C}$ . Equivalently,  $\phi(n)$  is the number of elements of order  $n$  in the cyclic group of order  $n$  (see Rotman Theorem 2.33(i)). Counting the elements of  $C_n$  (or counting  $n$ th roots of unity in  $\mathbb{C}$ ) gives you the useful equation

$$n = \sum_{d|n} \phi(d).$$

Now suppose that  $G$  is a group of order  $n$  with at most one cyclic subgroup of order  $d$  for each divisor  $d$  of  $n$ . It follows that  $G$  has at most  $\phi(d)$  elements of order  $d$  for each *proper* divisor  $d$  of  $n$ . Hence since  $n$  is the sum over all divisors  $d$  of  $n$  of the number of elements of  $G$  of order  $d$ , you see that

$$n \leq \sum_{d|n, d < n} \phi(d) + x \leq x + n - \phi(n)$$

where  $x$  is the number of elements of  $G$  of order  $n$ . It follows that  $x \geq \phi(n) > 0$ . Hence  $G$  has elements of order  $n$  so  $G$  is cyclic.

(iii) Remember that a polynomial  $f(x) \in K[x]$  of degree  $n$  has at most  $n$  roots in  $K$ . This is proved by induction on  $n$ , the base case  $n = 1$  being obvious. For the induction step, take  $f(x) \in K[x]$  of degree  $n$ . If  $f(x)$  has no roots in  $K$  we're done at once. So pick  $a \in K$  such that  $f(a) = 0$ . Using the division algorithm, we write

$$f(x) = (x - a)g(x) + r$$

for  $r \in K$ . Evaluating both sides at  $x = a$  proves that  $r = 0$ . Hence  $f(x) = (x - a)g(x)$ . Hence the number of roots of  $f(x)$  in  $K$  is at most one more than the number of roots of  $g(x)$  in  $K$ . So its  $\leq 1 + (n - 1) = n$  by the induction hypothesis.

(iv) We'll apply (ii). We just need to show that  $G$  has at most one cyclic subgroup of order  $d$  for each divisor  $d$  of  $n = |G|$ . Well suppose  $G$  has more than one cyclic subgroup of order  $d$  for some  $d|n$ . Then the equation  $x^d - 1$  has more than  $d$  solutions in  $K$  ( $d$  solutions from the first subgroup plus one more from something in the second but not the first subgroup). This contradicts (iii).

10. A *commutator* in a group  $G$  is an element of the form  $[g, h] = ghg^{-1}h^{-1}$  for  $g, h \in G$ .

(i) Let  $G'$  denote the subgroup of  $G$  generated by all commutators  $\{[g, h] \mid g \in G, h \in H\}$ . Prove that  $G'$  is the smallest normal subgroup of  $G$  such that  $G/G'$  is abelian.

(ii) Explain how to define a functor ("abelianization") from the category **groups** to the category **ab** so that an object  $G$  maps to  $G^{ab} := G/G'$ .

(iii) Let  $G$  be a group and  $H$  be an abelian group. Show that the sets  $\text{Hom}_{\mathbf{groups}}(G, H)$  and  $\text{Hom}_{\mathbf{ab}}(G^{ab}, H)$  have the same size.

(iv) Compute  $G^{ab}$  for each of the groups  $G = S_n$  ( $n \geq 1$ ),  $A_n$  ( $n \geq 2$ ),  $C_n$  ( $n \geq 1$ ) and  $D_n$  ( $n \geq 1$ ).

(i) Let's first check that  $G/G'$  is abelian. Well take  $g, h \in G$ . Then in  $G/G'$  we have that  $[gG', hG'] = [g, h]G'$  which is  $G'$  since  $[g, h] \in G'$ . Hence the cosets  $gG'$  and  $hG'$  commute because their commutator is zero.

Conversely, if  $N$  is any normal subgroup of  $G$  such that  $G/N$  is abelian, we need to show that  $G' \subseteq N$ . Well, arguing like in (i), we have for any  $g, h \in G$  that  $[g, h] \in N$ . Done.

(ii) If  $f : G \rightarrow H$  is a morphism,  $f$  maps each commutator in  $G$  to a commutator in  $H$ . Hence  $f$  maps  $G'$  into  $H'$ . Hence  $f$  induces a well defined map  $f^{ab}$  from  $G/G'$  to  $H/H'$ . Now we've defined the functor on both objects and morphisms we're done.

(iii) I'll define a bijection between these sets. Given  $f \in \text{Hom}_{\text{groups}}(G, H)$  with  $H$  abelian, note that the kernel of  $f$  is a normal subgroup such that the quotient  $G/\ker f$  is abelian. Hence,  $G' \subseteq \ker f$ . Hence  $f$  factors through the quotient to induce a homomorphism  $\bar{f}: G/G' \rightarrow H$ . This gives a map  $f \mapsto \bar{f}$  from  $\text{Hom}_{\text{groups}}(G, H)$  to  $\text{Hom}_{\text{ab}}(G^{ab}, H)$ . On the other hand given any map  $g$  from  $G^{ab}$  to  $H$  we can define a map  $\tilde{g}$  from  $G$  to  $H$  by composing  $g$  with the canonical quotient map  $G \rightarrow G/G'$ . This gives a map  $g \mapsto \tilde{g}$  that is the two-sided inverse of the map  $f \mapsto \bar{f}$ . Hence they're bijections.

(iv) For  $S_n$ : if  $n \leq 2$  then  $(S_n)^{ab} = S_n$ ; if  $n \geq 3$  then  $(S_n)^{ab} = S_n/A_n \cong C_2$ . For  $A_n$  you get that  $(A_n)^{ab} = A_n$  for  $n \leq 3$ ,  $(A_n)^{ab} = 1$  for  $n \geq 5$ , and  $(A_4)^{ab} \cong C_3$ . Clearly  $(C_n)^{ab} \cong C_n$ . Finally  $(D_n)^{ab} \cong C_2$  if  $n$  is odd and  $(D_n)^{ab} \cong V_4$  if  $n$  is even.

11. Recall that the direct product  $H \times K$  of two groups is just the Cartesian product with coordinatewise multiplication. It is sometimes called the "external" direct product since we have built a completely new group out of the two groups we started with. This is different from the notion of an "internal" direct product. A group  $G$  is said to be the *internal direct product* of  $H$  and  $K$  if  $H$  and  $K$  are subgroups of  $G$  and the map  $H \times K \rightarrow G, (h, k) \mapsto hk$  is an isomorphism.

(i) Prove that  $G$  is the internal direct product of  $H$  and  $K$  if and only if  $H \trianglelefteq G, K \trianglelefteq G, G = HK$  and  $H \cap K = \{1\}$ .

(ii) For which  $n$  is the dihedral group  $D_n$  an internal direct product of two proper subgroups?

(i) If  $G = H \times K$  it is clear that  $H = H \times 1$  and  $K = 1 \times K$  satisfy  $H \trianglelefteq G, K \trianglelefteq G, G = HK$  and  $H \cap K = \{1\}$ . Conversely if those conditions hold, consider the map  $H \times K \rightarrow G, (h, k) \mapsto hk$ . To check that it is a group homomorphism we need to show that  $hk = kh$  for all  $h \in H, k \in K$ . But their commutator  $hkh^{-1}k^{-1}$  lies in  $H \cap K = 1$  so yes. It is onto since  $G = HK$  and it is injective since its kernel is  $\cong H \cap K$ . Hence it is an isomorphism.

(ii) If  $n$  is even then  $D_n \cong D_{n/2} \times C_2$ . If  $n$  is odd it is not a proper direct product.

12. Suppose that  $K$  is a finite field with  $q$  elements.

(i) Explain why  $|GL_n(K)|$  is equal to the number of distinct ordered bases  $(v_1, \dots, v_n)$  for the vector space  $K^n$ . Hence compute  $|GL_n(K)|$  and  $|SL_n(K)|$ .

(ii) Suppose for the remainder of the question that  $V$  is a  $2n$ -dimensional vector space over  $K$  equipped with a non-degenerate skew-symmetric bilinear form. Explain why there are  $\frac{(q^{2n}-1)(q^{2n}-q^{2n-1})}{(q^2-1)(q^2-q)}$  different non-degenerate 2-dimensional subspaces of  $V$ .

(iii) Recall that  $Sp(V) \cong Sp_{2n}(K)$  is the group of all linear maps from  $V$  to  $V$  preserving the given non-degenerate skew-symmetric form. Prove that the stabilizer in  $Sp(V)$  of a non-degenerate 2-dimensional subspace is isomorphic to  $Sp_{2n-2}(K) \times Sp_2(K)$ . Hence deduce that

$$|Sp_{2n}(K)| = q^{n^2}(q^{2n}-1)(q^{2n-2}-1)\cdots(q^2-1).$$

(iv) How many *different* non-degenerate skew-symmetric bilinear forms are there on the vector space  $V$ ?

(i) Let  $GL_n(K)$  act on bases for  $K^n$  in the obvious way (by matrix multiplication). This action is transitive and the stabilizer of the standard basis is trivial. Hence  $|GL_n(K)|$  is the number of distinct bases. Now count... to pick a basis the first vector can be anything but 0,  $q^n - 1$  choices; the second can be anything outside the 1-space spanned by the first vector,  $q^n - q$  choices, ... We deduce

$$|GL_n(K)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}).$$

Then  $|SL_n(K)| = |GL_n(K)|/(q-1)$  since there are  $|K^\times| = (q-1)$  cosets of  $SL_n(K)$  in  $GL_n(K)$ .

(ii) To count non-degenerate 2-subspaces, we need to pick any non-zero vector  $v$ ,  $q^{2n} - 1$  ways, then any vector outside of  $v^\perp$ . Since  $v^\perp$  is of dimension  $(2n - 1)$ , there are  $q^{2n-1}$  vectors in  $v^\perp$ . Hence there are  $q^{2n} - q^{2n-1}$  ways to pick the second vector. Then we need to divide through by  $(q^2 - 1)(q^2 - q)$  since that is how many different bases a given non-degenerate 2-subspace has. We conclude there are  $(q^{2n} - 1)(q^{2n} - q^{2n-1})/(q^2 - 1)(q^2 - q)$  nondegenerate 2-subspaces, as required.

(iii) Let  $U$  be a non-degenerate 2-subspace, so  $V = U \oplus U^\perp$ . The stabilizer in  $Sp(V)$  of  $U$  also stabilizes  $U^\perp$ , hence it is contained in  $Sp(U) \times Sp(U^\perp)$ . On the other hand anything in the latter group does indeed lie in  $Sp(V)$  and stabilize  $U$ . Hence, the stabilizer is exactly  $Sp(U) \times Sp(U^\perp)$ . Now we can compute the order of  $Sp_{2n}(K)$  using (ii):

$$|Sp_{2n}(K)| = |Sp_{2n-2}(K)||Sp_2(K)| \times (q^{2n} - 1)(q^{2n} - q^{2n-1}) / (q^2 - 1)(q^2 - q).$$

This simplifies by induction to the given answer. I guess you have to know to start with that  $|Sp_2(K)| = q(q^2 - 1)$ , but that follows from (i) since  $Sp_2(K) = SL_2(K)$ ...

(iv) Let  $GL_{2n}(K)$  act on non-degenerate skew-symmetric forms on  $V$  by letting  ${}^g(\cdot, \cdot)$  be the form defined by  ${}^g(v, w) = (gv, gw)$ . The action is transitive (because all non-degenerate skew-symmetric forms have a basis in which they look the same...) and the stabilizer of a given form is  $Sp_{2n}(K)$ . Hence the number of forms is  $[GL_{2n}(K) : Sp_{2n}(K)]$  which you can compute using (i) and (iii) to get: there are

$$(q^{2n-1} - 1)(q^{2n-1} - q^2) \cdots (q^{2n-1} - q^{2n-2})$$

different non-degenerate skew-symmetric forms on  $V$ .

13. Prove that there is no simple group of order 120.

We have  $120 = 2^3 \cdot 3 \cdot 5$ . So there are 6 Sylow 5 subgroups. The conjugation action on the Sylow 5-subgroups yields an embedding of  $G$  into  $S_6$ . By simplicity of  $G$  we have  $G \leq A_6$ , and  $[A_6 : G] = 3$ . But  $A_6$  does not have subgroups of index 3, as it is simple and therefore cannot act transitively on a three element set.

14. Suppose that  $G$  is a group of order  $p^3q$  for distinct primes  $p, q$  and that  $G$  has no normal Sylow subgroups. Compute  $|G|$ . Give an example of such a group.

We have that  $n_p, n_q > 1$ . Hence by Sylow theorems  $n_p = q > p$  and  $n_q$  equals  $p, p^2$  or  $p^3$ . Can't have  $n_q = p$  as  $q > p$ . Can't have  $n_q = p^3$ . If it was, then we would have  $p^3(q-1)$  elements of order  $q$  leaving room for just  $p^3$  more elements, i.e. a unique Sylow  $p$ -subgroup. So we must have that  $n_q = p^2$ . Hence  $q|(p^2 - 1)$ . So  $q|(p+1)$ . So  $q = p+1$  as  $q > p$ . But both  $p$  and  $q$  are prime. So  $q = 3, p = 2$  and  $|G| = 24$ . The example is  $S_4$ .

15. Let  $p, q, r$  be distinct primes. Prove that there are no simple groups of order  $pqr$ .

Suppose  $p > q > r$ . We have that  $n_p = qr$ . Thus there are  $(p-1)qr$  elements of order  $p$ . Similarly we must have that  $n_q \geq p$  and  $n_r \geq q$ . Hence there are  $\geq (q-1)p + (r-1)q$  elements of orders  $q$  and  $r$ . Thus there are at least

$$pqr - qr + pq - p + qr - q + 1 = pqr + (p-1)(q-1) > pqr$$

elements in  $G$ . This is a contradiction.

16. Suppose that  $G$  is a non-abelian simple group with  $|G| < 200$ . Prove that  $|G| = 60$  or  $|G| = 168$ . *To make life easier - though you can solve this without it - you may assume without proof the following consequence of Burnside's  $p^a q^b$  theorem which we will discuss later in the course: there is no simple group of order  $p^a q^b$  for  $p, q$  distinct primes.*

This is a lengthy case analysis. Almost everything is accounted for by problem 15 or Burnside. The remainder you need ad hoc arguments like question 13. Perhaps the hardest case you get to look at is groups of order 180. Here is the ad hoc argument to show there are no simple groups of order 180...

Since  $180 = 2^2 \cdot 3^2 \cdot 5$  we get that  $n_5 = 1, 6$  or  $36$ . If  $n_5 = 1$  we're done, its got a normal Sylow 5 so its not simple. If  $n_5 = 6$  then the conjugation action of  $G$  on Sylow 5 subgroups gives us a homomorphism from  $G$  to  $S_6$ , hence if  $G$  is simple  $G$  embeds as a subgroup of order 180 of the alternating group  $A_6$  of order 360. But  $A_6$  has no subgroup of index 2 as  $A_6$  is simple. So this doesn't happen. Hence,  $n_5 = 36$ . This means that  $G$  has a total of  $4 \cdot 36 = 144$  elements of order 5, leaving just 36 more elements of order different from 5.

Now consider  $n_3$ . It is 1, 4 or 10. If it is 1,  $G$  is not simple, and if it is 4 then  $G$  maps to  $S_4$  hence its kernel is a non-trivial normal subgroup of  $G$  and  $G$  is not simple. Hence  $n_3 = 10$ . Note Sylow

3-subgroup is of order 9 so it is certainly abelian. Let  $P$  and  $Q$  be two Sylow 3-subgroups such that  $P \cap Q \neq 1$ . Consider the normalizer  $N$  in  $G$  of  $P \cap Q$ . It contains  $P$  and  $Q$ , hence it is a subgroup of  $G$  of order dividing 180, divisible by 9 and strictly bigger than 9. It cannot be 18, for then  $P$  and  $Q$  would both be distinct normal Sylow  $p$ -subgroups of  $N$ . This only leaves 36, 45 or 90. Hence  $[G : N] \leq 5$ . So we get a map from the action of  $G$  on cosets of  $N$  from  $G$  to  $S_5$ . It has a kernel giving a normal subgroup of  $G$ .

It just remains to look at the possibility that  $P \cap Q = 1$  for all pairs  $P, Q$  of Sylow 3-subgroup. In that case we get at least 80 elements of order 3 or 9 in  $G$ , and there is not room for that...

17. Suppose that  $G$  is a simple group of order 60. Prove that  $G \cong A_5$ .

Since  $60 = 2^2 \cdot 3 \cdot 5$  we get that  $n_5 = 1$  or 6. It cannot be 1 as  $G$  is simple. Hence,  $n_5 = 6$  and  $G$  has 24 elements of order 5, leaving room for just 36 more elements of order  $\neq 5$ .

Consider  $n_2 = 1, 3, 5$  or 15. It cannot be 1 (then it has a normal Sylow 2 subgroup), it cannot be 3 (then  $G$  maps to  $S_3$  giving a kernel contradicting simplicity). So it is 5 or 15. If it is 5 then we get a map from  $G$  to  $S_5$ , hence an isomorphism between  $G$  and  $A_5$  if  $G$  is simple. Therefore we just need to rule out the possibility that  $n_2 = 15$ .

Let  $P$  and  $Q$  be Sylow 2-subgroups with  $P \cap Q \neq 1$ . Let  $N$  be the normalizer in  $G$  of  $P \cap Q$ . So  $N$  contains both  $P$  and  $Q$ , hence  $|N|$  divides 60 and is divisible by but strictly bigger than 4. Hence  $|N| = 12, 20$  or 60. Its not the whole group as  $G$  is simple. Its not 20 since then  $G$  has a subgroup of index 3, whence a map  $G \rightarrow S_3$  contradicting simplicity. So  $|N| = 12$ . This gives us a subgroup of index 5, hence an injective map from  $G$  to  $S_5$  by action on the cosets of  $N$ . Since  $G$  is simple this means  $G$  maps isomorphically onto  $A_5 < S_5$ . But this is a contradiction since  $A_5$  has  $n_2 = 5$ .

It follows that  $P \cap A = 1$  for all Sylow 2-subgroups. But this gives  $15 \times 3 = 45$  elements of order 2 or 4, and there is not room for that.... So  $n_2 = 15$  has been ruled out.

18. Recall a permutation group  $G$  acting on a set  $X$  is *transitive* if for each  $x, y \in X$  there exists  $g \in G$  with  $gx = y$ . Instead,  $G$  is called *2-transitive* if for each  $x_1 \neq x_2$  and  $y_1 \neq y_2$  from  $X$  there exists  $g \in G$  with  $gx_1 = y_1, gx_2 = y_2$ .

(i) Show that  $A_n$  is a 2-transitive permutation group on  $\{1, \dots, n\}$  for  $n \geq 4$ .

(ii) If  $G$  is a 2-transitive permutation group on  $X$  and  $1 < K \trianglelefteq G$ , prove that  $K$  is transitive on  $X$ .

(i) Let  $x_1 \neq x_2$  and  $y_1 \neq y_2$  be chosen from  $\{1, \dots, n\}$ . Its obvious that  $A_n$  is transitive for  $n \geq 3$  (e.g. 3-cycles). So we can pick  $h \in A_n$  with  $hx_1 = y_1$ . Then  $h^{-1}y_2 \neq x_1$  (if it did then  $y_1$  would equal  $y_2$ ). Now consider  $\{1, \dots, n\} - \{x_1\}$ , which contains  $x_2$  and  $h^{-1}y_2$ . The stabilizer in  $A_n$  of  $x_1$  is  $A_{n-1}$ , which is transitive on  $\{1, \dots, n\} - \{x_1\}$ , so we can find an element  $g$  in this stabilizer such that  $gx_1 = x_1$  and  $gx_2 = h^{-1}y_2$ . Then  $hgx_1 = y_1$  and  $hgx_2 = y_2$ .

(ii) Take  $x, y \in X$ . We need to find  $k \in K$  such that  $kx = y$ . Suppose first that  $kx = x$  for all  $k \in K$ . Pick any other  $z \in X$  and  $g \in G$  such that  $gx = z$ . Then  $g^{-1}kgx = x$  hence  $kz = z$  for all  $k \in K$ . This means that every element of  $k$  fixes every element of  $X$ , i.e.  $K = 1$  which is not the case. So we can fix  $k \in K$  such that  $kx = z \neq x$ . Now pick  $g \in G$  such that  $gx = x$  and  $gy = z$ , which we can do as  $G$  is 2-transitive. Then  $(g^{-1}kg)x = y$  as required.

19. The goal of this problem is to prove that the group  $G = GL_3(\mathbb{F}_2)$  of  $3 \times 3$  invertible matrices over the field with two elements is a simple group.

(i) What is the order  $|G|$ ?

(ii) Let  $V = (\mathbb{F}_2)^3$  be the vector space that  $G$  acts on naturally. Prove that  $G$  acts 2-transitively on  $V - \{0\}$ .

(iii) Hence by question 18 if  $1 < K \trianglelefteq G$  then  $K$  is transitive on  $V - \{0\}$ . Deduce that  $7 \mid |K|$ .

(iv) Now let  $n_7$  denote the number of Sylow 7-subgroups of  $K$ , so  $n_7 = 1$  or  $n_7 = 8$ . If  $n_7 = 8$  and  $K \neq G$  prove that  $K$  has a unique Sylow 2-subgroup. Why does this imply that  $G$  itself has a unique Sylow 2-subgroup too? Obtain a contradiction by exhibiting more than one Sylow 2-subgroup in  $G$  explicitly.

(v) If  $n_7 = 1$  then  $G$  has just 6 elements of order 7. Obtain a contradiction. Hence  $G$  is simple.

(i) 168.

(ii) Take non-zero vectors  $v_1 \neq v_2$  and  $w_1 \neq w_2$ . Since the ground field is  $\mathbb{F}_2$ ,  $v_2$  is not a scalar multiple of  $v_1$ . Hence  $v_1$  and  $v_2$  are linearly independent. Similarly  $w_1$  and  $w_2$  are linearly independent. Extend to bases  $v_1, v_2, v_3$  and  $w_1, w_2, w_3$  for  $V$ . Let  $g$  be the matrix with columns  $v_1, v_2, v_3$  and let  $h$  be the matrix with columns  $w_1, w_2, w_3$ . These both belong to  $GL_3(\mathbb{F}_2)$  since their columns are linearly independent. Then  $hg^{-1}$  sends  $v_1, v_2, v_3$  to  $w_1, w_2, w_3$ . So it is certainly 2-transitive.

(iii) Note  $V - \{0\}$  is a set of order 7. So since size of orbit divides size of group and  $K$  has an orbit of size 7, we have that  $7 \mid |K|$ .

(iv) If  $n_7 = 8$  then  $K$  has 48 elements of order 7. The order of  $K$  is a proper divisor of 168 and it must be divisible by 7 and by 8 hence by 56. Hence  $|K| = 56$ . So there are just 8 elements of order different from 7. Therefore there is a unique Sylow 2-subgroup in  $K$ . But then it is also normal in  $G$ , so  $G$  has a unique Sylow 2-subgroup too. But take the upper unitriangular matrices: that is a subgroup of order 8 hence a Sylow 2-subgroup. On the other hand the lower unitriangular matrices is another such. We've exhibited two Sylow 2-subgroups. Contradiction.

(v) So we are left with  $n_7 = 1$ . Hence  $G$  has a unique Sylow 7-subgroup, and just 6 elements of order 7. Here are two ways to get the contradiction...

Method one. Consider the matrices

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

These satisfy  $A^3 + A^2 + 1 = 0$  (here's how to see it without multiplying matrices:  $Ae_1 = e_2, Ae_2 = e_3, Ae_3 = e_1 + e_3$  hence  $(A^3 + A^2 + 1)e_1 = 0$  now multiply by  $A$  to get that  $(A^3 + A^2 + 1)e_i = 0$  for all  $i$ ) and  $B^3 + B + 1 = 0$ . Since  $x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$  in the ring  $\mathbb{F}_2[x]$  it follows that  $A^7 = B^7 = 1$ , so they are elements of order 7. But  $A$  is not a power of  $B$ . So  $B, B^2, B^3, B^4, B^5, B^6, A$  give us 7 elements of order 7. Contradiction.

Method two. Let  $Q$  be the Sylow 7-subgroup of  $G$ . Let  $G$  act on  $Q - \{1\}$  by conjugation. Let  $1 \neq q \in Q$ . We have that the size of the conjugacy class of  $q$  is at most 6, i.e.  $[G : C_G(q)] \leq 6$ . So  $|C_G(q)| \geq 28$ . But the action of  $G$  on  $V^*$  is faithful so  $G$  embeds as a subgroup of  $S_7$ . In  $S_7$  the centralizer of a 7 cycle is the subgroup of order 7 generated by that 7 cycle. So  $|C_G(q)| \leq 7$ . Contradiction.

20. For any field  $k$ , prove that  $GL_n(k)$  is a semidirect product of  $SL_n(k)$  by  $k^\times$ .

We know already that  $GL_n(k)$  is an extension

$$1 \rightarrow SL_n(k) \rightarrow GL_n(k) \rightarrow k^\times \rightarrow 1.$$

We need to show that the right hand map (determinant) is split. Define a splitting  $k^\times \rightarrow GL_n(k)$  mapping  $c$  to the matrix  $\text{diag}(c, 1, 1, \dots, 1)$ .

Note it is usually not the direct product. For example if  $GL_2(\mathbb{R})$  was the direct product it would have a normal subgroup isomorphic to  $\mathbb{R}^\times$ ; the only possibility is the scalar matrices  $\{\text{diag}(c, c) \mid c \in \mathbb{R}^\times\}$ . But that doesn't intersect  $SL_2(\mathbb{R})$  trivially:  $\text{diag}(-1, -1)$  is in the intersection.

21. Let  $G$  be the subgroup of  $GL_2(\mathbb{C})$  generated by the matrices

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

where  $\omega = e^{2\pi i/3}$  is a primitive cube root of unity. Prove that  $G$  is a group of order 12 that is not isomorphic to  $A_4$  or  $D_6$ .

Multiplying matrices, you see that  $G$  consists of the following 12 matrices:

$$\begin{aligned} & \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ & \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & i\omega \\ i\omega^2 & 0 \end{pmatrix} \\ & \begin{pmatrix} -\omega & 0 \\ 0 & -\omega^2 \end{pmatrix}, \quad \begin{pmatrix} 0 & i\omega^2 \\ i\omega & 0 \end{pmatrix} \\ & \begin{pmatrix} -\omega^2 & 0 \\ 0 & -\omega \end{pmatrix}, \quad \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \\ & \begin{pmatrix} 0 & -i\omega \\ -i\omega^2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -i\omega^2 \\ -i\omega & 0 \end{pmatrix}. \end{aligned}$$

Now note that  $\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$  generates a normal subgroup of order 3 and  $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$  generates a subgroup of order 4 isomorphic to  $C_4$ . It must be a non-abelian semidirect product of these two, i.e.  $G = C_3 \rtimes C_4$ .

To see this is not isomorphic to  $A_4$  note our group has an element of order 6, but  $A_4$  does not. And  $D_6 = S_3 \times C_2$  has no element of order 4 but our group has.

22. Recall that the *quaternions*  $\mathbb{H}$  are defined to be the real vector space of dimension 4 with basis  $1, i, j, k$  with associative, bilinear multiplication (making it into a ring or more precisely an  $\mathbb{R}$ -algebra with identity element 1) defined on the basis elements by  $i^2 = j^2 = k^2 = -1$ ,  $ij = k$ ,  $jk = i$  and  $ki = j$ .

(i) Prove that every non-zero quaternion is a unit with inverse

$$(a + bi + cj + dk)^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk).$$

Hence  $\mathbb{H}$  is a *division algebra* (a non-commutative field).

(ii) Define the *norm*  $N : \mathbb{H}^\times \rightarrow \mathbb{R}^+$  by  $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$ . Check that this is a group homomorphism and moreover every  $h \in \mathbb{H}^\times$  has a *polar decomposition*  $h = rs$  where  $r \in \mathbb{R}^+$  and  $s \in \ker N$  (which is the sphere  $S^3$ !).

(iii) Let  $A$  be the set of all matrices of the form  $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$  where  $z$  and  $w$  are complex numbers and  $z \mapsto \bar{z}$  denotes complex conjugation. Prove that  $A$  is a subring of the ring  $M_2(\mathbb{C})$  of  $2 \times 2$  complex matrices and that  $A \cong \mathbb{H}$ .

(iv) Using your answer to (iii), prove that the normal subgroup  $\ker N$  of  $\mathbb{H}^\times$  is isomorphic to the group  $SU(2)$  – the *special unitary group* consisting of all  $2 \times 2$  complex matrices  $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$  of determinant 1 such that  $p\bar{q} + r\bar{s} = 0$  and  $p\bar{p} + r\bar{r} = 1 = q\bar{q} + s\bar{s}$ .

(v) Deduce that  $\mathbb{H}^\times = SU(2) \rtimes \mathbb{R}^+$ .

(i) Just multiply.

(ii) Again you have to check by expanding everything. The polar decomposition is  $h = N(h)\left(\frac{h}{N(h)}\right)$ .

(iii) Define a linear map  $\mathbb{H} \rightarrow M_2(\mathbb{C})$  by mapping the basis element 1 to the identity matrix and

$$\begin{aligned} i & \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \\ j & \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \\ k & \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}. \end{aligned}$$

The image of this map is obviously the given set  $A$ . Moreover it is a ring homomorphism. To check this you just have to show that these three matrices square to  $-1$  and they satisfy the relations corresponding to  $ij = k, jk = i$  and  $ki = j$ . Everything else follows as matrix multiplication is bilinear.

(iv) If you identify  $\mathbb{H}$  and  $A$  via the map in (iii) the norm map  $N$  corresponds to the determinant map... So  $\ker N$  is the subgroup of  $A$  consisting of all such matrices of determinant 1. It is easy to see that all these guys lie in  $SU(2)$ .

Conversely take  $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$  in  $SU(2)$  satisfying

$$p\bar{q} + r\bar{s} = 0,$$

$$ps - qr = 1,$$

$$p\bar{p} + r\bar{r} = 1,$$

$$q\bar{q} + s\bar{s} = 1.$$

We need to show that  $\bar{s} = p$  and  $q = -\bar{r}$ ... It is easy enough to see that if  $p = 0$  then you must also have  $s = 0$  and  $q = -\bar{r}$ . Now suppose  $p \neq 0$ . From the first equation you get that

$$q = -\frac{\bar{r}s}{|p|^2}.$$

Substituting into the second equation gives that

$$s = \frac{\bar{p}}{|p|^2 + |s|^2}.$$

Hence in fact

$$q = -\frac{\bar{r}}{|p|^2 + |s|^2}.$$

We're just left with proving that  $|p|^2 + |s|^2 = 1$ . But this follows by substituting  $s$  and  $q$  into the final equation.

(v) By (ii) we have that  $\mathbb{H}^\times = \ker N \rtimes \mathbb{R}^\times$ . By (iv)  $\ker N \cong SU(2)$ . So we're done.

23. Recall that the quaternion group  $Q_3$  is the subgroup  $\{\pm 1, \pm i, \pm j, \pm k\}$  of  $\mathbb{H}^\times$ .

(i) Prove that  $Q_3$  is isomorphic to the group  $\langle x, y \mid x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$ .

(ii) Prove that  $Q_3$  is not isomorphic to the semidirect product  $C_4 \rtimes C_2$  of a cyclic group of order 4 by a cyclic group of order 2. Deduce that  $Q_3 \not\cong D_4$ .

(i) Let  $G = \langle x, y \mid x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$ . Every word in  $x, y$  can be reduced using the relations to the form  $x^i y^j$  for  $i = 0, 1, 2, 3$  and  $j = 0, 1$ . Hence  $|G| \leq 8$ . The elements  $i$  and  $j$  in  $Q_3$  satisfy the same relations as  $x$  and  $y$ . Hence by the universal property of free groups, there is a group homomorphism  $G \rightarrow Q_3$ . Since  $i$  and  $j$  generate  $Q_3$  this is onto. Since  $|Q_3| = 8$  and  $|G| \leq 8$  it must actually be an isomorphism.

(ii) The only element of order 2 in  $Q_3$  is the element  $-1$ . The elements of order 4 are  $\pm i, \pm j$  and  $\pm k$ . Hence  $-1$  lies in every  $C_4$  subgroup. So there is no way it can be a semidirect product of  $C_4$  by  $C_2$  – there could be no possible splitting. Since  $D_4 = C_4 \rtimes C_2$  (where the  $C_4$  is the rotation subgroup and the  $C_2$  is a reflection subgroup) this means that  $Q_3 \not\cong D_4$ .

24. Let  $G$  be a finite group,  $N \trianglelefteq G$  and  $P$  be a Sylow  $p$ -subgroup of  $G$  for some prime  $p$ . Prove that  $PN/N$  is a Sylow  $p$ -subgroup of  $G/N$  and  $P \cap N$  is a Sylow  $p$ -subgroup of  $N$ .

For the first one, we just have to show that  $p \nmid [G/N : PN/N]$ . But  $[G/N : PN/N] = [G : PN]$  which divides  $[G : P]$ , and  $p \nmid [G : P]$ .

For the second one, we have to show that  $p \nmid [N : P \cap N]$ . But  $[N : P \cap N] = [PN : P]$  which again divides  $[G : P]$  etc...

25. Prove that all of the following groups are abelian:

(i) A group  $G$  all of whose elements are of order 1 or 2.

(ii) A group  $G$  with  $|\text{Aut}(G)| = 1$ .

(iii) A group  $G$  of order  $p^2$  ( $p$  prime).

(i)  $(xy)^2 = 1$ . Hence  $xyxy = 1$ . Hence  $xyxyxy = xy$ . Hence  $yx = xy$ .

(ii) Define a map  $G \rightarrow \text{Aut}(G), g \mapsto \gamma_g$  where  $\gamma_g(x) = gxg^{-1}$ . Since  $|\text{Aut}(G)| = 1$  we get that  $gxg^{-1} = x$  for all  $g \in G, x \in G$ . Hence  $G$  is abelian. (In fact the only such groups  $G$  are the groups of order  $\leq 2$ !!!)

(iii) If  $G$  contains an element of order  $p^2$  it is cyclic and we are done already. So we may assume that all non-identity elements of  $G$  are of order  $p$ .

By the class equation we have that  $|G| \equiv |Z(G)| \pmod{p}$ . Hence  $|Z(G)|$  is of order  $p$  or  $p^2$ . In the latter case we are done again. So we may assume that  $|Z(G)| = p$ .

But now take any element  $g$  of  $G - Z(G)$ . Consider  $C_G(g)$ . It contains  $Z(G)$  and  $g$ , hence by Lagrange's theorem  $C_G(g) = G$ . But this means that  $g \in Z(G)$ . Contradiction.

26. Let  $p$  be a prime. How many subgroups does the group  $C_p \times C_p$  have? (Don't forget the trivial ones!)

It is the same as the number of subspaces of the two dimensional vector space  $(\mathbb{F}_p)^2$ . There are  $(p + 1)$  one dimensional ones plus 2 more.

27. How many different groups of order 18 are there up to isomorphism? (There are only two groups of order 9, namely,  $C_9$  and  $C_3 \times C_3$ .)

By Sylow theorems we have that  $n_3 = 1$ . Hence there's a normal Sylow 3-subgroup. There's also a  $C_2$ -subgroup. So it must be a direct product (if the  $C_2$  is normal) or a semidirect product (if the  $C_2$  is not normal). Direct products give us  $C_3 \times C_3 \times C_2$  and  $C_9 \times C_2$ . That is two so far. Now we're left with the non-abelian either  $(C_3 \times C_3) \rtimes C_2$  or  $C_9 \rtimes C_2$ .

We still have to think about the automorphisms of  $C_3 \times C_3$  and of  $C_9$  of order 2 to work out exactly how many different semidirect products there are of each type (up to isomorphism). In the second case, viewing  $C_9$  as  $\mathbb{Z}_9$ , its automorphism group is  $\mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$ . The only elements of this of order 2 are 2 and 5. So the only automorphism of order 2 swaps 2 and 5, and there is just one possibility. So there is just one group looking like  $C_9 \rtimes C_2$ , namely, the dihedral group  $D_9$ .

Finally for  $C_3 \times C_3$ , view it as  $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ . Then automorphisms are given by invertible  $2 \times 2$  matrices with entries in  $\mathbb{Z}_3$ . Since we only care up to isomorphism, we only need to worry about such matrices up to conjugation. Since  $x^2 - 1 = 0$  the minimal polynomial has distinct roots so such matrices are diagonalizable. So there are just two possibilities to worry about:  $\text{diag}(1, -1)$  and  $\text{diag}(-1, -1)$ .

This gives two more candidates, the first is  $(C_3 \times C_2) \times C_3 = S_3 \times C_3$  which has a central  $C_3$ . The second is  $(C_3 \times C_3) \rtimes C_2$  where the non-identity element of the  $C_2$  is acting by  $g \mapsto g^{-1}$ . There is no element of order 3 centralized by this. So the center is trivial in this case. So it is different from the first one.

Conclusion: 5 groups of order 18 up to isomorphism.

28. We will prove in class that  $PSL_2(\mathbb{F}_5)$ , the quotient of the special linear group  $SL_n(\mathbb{F}_5)$  by its center  $\{\pm I_2\}$ , is a simple group of order 60. Hence it is isomorphic to the group  $A_5$ . Prove that  $SL_2(\mathbb{F}_5)$  is a non-split extension of  $C_2$  by  $A_5$ .

The center of  $SL_2(\mathbb{F}_5)$  is a normal subgroup isomorphic to  $C_2$  with quotient isomorphic to  $A_5$ . So  $SL_2(\mathbb{F}_5)$  is an extension of  $C_2$  by  $A_5$ . To show that the extension is non-split, note that  $SL_2(\mathbb{F}_5)$  contains elements of order 4 (e.g.  $\text{diag}(2, 3)$ ) but  $A_5$  has no elements of order 4. If the extension was split then every element could be written as  $\pm x$  for  $x \in A_5$ . But no such element can have order 4: if  $(\pm x)^4 = 1$  then  $x^4 = 1$  in  $A_5$  so  $x^2 = 1$  already. But then  $(\pm x)^2 = 1$  already and it is of order 2...

29. Suppose that  $G$  and  $H$  are finite groups with  $(|G|, |H|) = 1$ . Is it true that every subgroup of  $G \times H$  is of the form  $G' \times H'$  for  $G' \leq G$  and  $H' \leq H$ ?

YES. Let  $K$  be a subgroup of  $G \times H$ . Consider the projections  $\pi_G : G \times H \rightarrow G$  and  $\pi_H : G \times H \rightarrow H$ . Let  $G' = \pi_G(K)$ ,  $H' = \pi_H(K)$ . It is obvious that  $K \leq G' \times H'$ . Conversely, we show that  $G' \times H' \leq K$ . Take  $(g, h) \in G' \times H'$ . This means that  $(g, h') \in K$  and  $(g', h) \in K$  for some  $g' \in G, h' \in H$ . Now I claim that  $(g, h') \in K$  implies  $(g, 1) \in K$ . Similarly,  $(g', h) \in K$  implies  $(1, h) \in K$ . Hence we'll get that  $(g, h) \in K$  too, so that  $G' \times H' \leq K$  as required to finish the argument.

To prove the claim, suppose  $(g, h') \in K$ . Let  $n = |H|$ . Then  $(g, h')^n = (g^n, 1)$ . So  $(g^n, 1) \in K$ . But the order of  $g$  divides  $|G|$ , which is prime to  $n$ . It follows that  $g^n$  generates the same subgroup of  $G$  as  $g$  does. Hence  $(g^n, 1) \in K$  implies  $(g, 1) \in K$ . We're done.

30. Let  $1 < m < n - 1$ , and  $G$  be the symmetric group  $S_n$  acting on the set  $X$  of  $m$ -element subsets of  $\{1, \dots, n\}$ .

(i) Show that  $G$  is not 2-transitive on  $X$ .

(ii) What is the stabilizer of a point?

(iii) Using your answer to (ii) determine for which  $m$  the action of  $G$  on  $X$  is primitive.

(i) Just consider the sets  $X = \{1, \dots, m\}$ ,  $Y = \{1, \dots, m-1, m+1\}$  and  $Z = \{2, \dots, m+1\}$ . You cannot send the pair  $(X, Y)$  to the pair  $(X, Z)$ .

(ii) The stabilizer of the point  $\{1, \dots, m\}$  is the product  $S_m \times S_{n-m}$  of the symmetric group  $S_m$  on  $\{1, \dots, m\}$  and the symmetric group  $S_{n-m}$  on  $\{m+1, \dots, n\}$ .

(iii) The action is primitive if and only if  $S_m \times S_{n-m}$  is a maximal subgroup of  $S_n$ .

If  $m = n/2$  then  $S_m \times S_m$  is not maximal in  $S_{2m}$ : it is contained in the wreath product  $(S_m \times S_m) \rtimes S_2$ .

But if  $m \neq n/2$  it is maximal, hence the action is primitive. Proof. WLOG  $m > n/2$ . Take  $g \notin S_m \times S_{n-m}$ . I will show  $S_m \times S_{n-m}$  and  $g$  together generate all of  $S_n$ . It suffices to show any transposition lies in the subgroup of  $S_n$  generated by  $S_m \times S_{n-m}$  and  $g$ . Transpositions  $(ij)$  for  $i, j \in \{1, \dots, m\}$  or  $i, j \in \{m+1, \dots, n\}$  are obviously there. So we need to get transpositions  $(ij)$  for  $i \in \{1, \dots, m\}$  and  $j \in \{m+1, \dots, n\}$ . It is enough to get just one of these, then we can conjugate by  $S_m \times S_{n-m}$  to get all the others.

Well, since  $g \notin S_m \times S_{n-m}$ , I can find  $i \in \{1, \dots, m\}$  and  $j \in \{m+1, \dots, n\}$  such that  $g(i) = j$ . Since  $m > n/2$ , I can also find  $p, q \in \{1, \dots, m\}$  such that  $g(p) = q$ . (There is no room to map everything from  $\{1, \dots, m\}$  to  $\{m+1, \dots, n\}$ !). Now consider

$$g(ip)g^{-1} = (jq).$$

It's a transposition that we were after...

31. This exercise is concerned with a useful counterexample! Let  $p$  be a prime and define the group  $C_{p^\infty}$  to be the subgroup of  $\mathbb{C}^\times$  consisting of all  $p^n$ th roots of 1 for all  $n \geq 0$ . Note that  $C_{p^\infty}$  is an example of an infinite  $p$ -group: all its elements are of order a power of  $p$ .

(i) Let  $C_p$  denote the subgroup of  $C_{p^\infty}$  consisting of all  $p$ th roots of 1. By considering the map  $z \mapsto z^p$ , prove that  $C_{p^\infty}/C_p \cong C_{p^\infty}$ .

(ii) Prove that every finitely generated subgroup of  $C_{p^\infty}$  is cyclic, but  $C_{p^\infty}$  is not cyclic itself.

(iii) (An alternative definition.) By considering the map  $q \mapsto e^{2\pi i q}$ , prove that  $C_{p^\infty}$  is isomorphic to the subgroup  $\{\frac{a}{p^n} \mid a \in \mathbb{Z}, n \geq 0\}$  of the quotient group  $\mathbb{Q}/\mathbb{Z}$  (rational numbers modulo 1).

(i) The kernel of the given map is  $C_p$ . So all you have to see is that the image is everything. I think it's clear.

(ii) Take a finitely generated subgroup of  $C_{p^\infty}$ . Say the generators of the subgroup are  $g_1, \dots, g_n$  of orders  $p^{r_1}, \dots, p^{r_n}$ . Let  $r = \max(r_1, \dots, r_n)$ . Then every generator satisfies  $g^{p^r} = 1$ . So every generator is a  $p^r$ -th root of 1, hence is a power of the generator of order  $p^r$  since that is a primitive  $p^r$ -th root of 1. This shows our group is just the cyclic group of order  $p^r$ .

(iii) There is a homomorphism from the abelian group  $\mathbb{Q}$  to the circle group  $S^1$  mapping  $q$  to  $e^{2\pi i q}$ . The kernel is  $\mathbb{Z}$ . So  $\mathbb{Q}/\mathbb{Z}$  embeds into  $S^1$  as the elements of finite order. Now just see what  $C_{p^\infty}$  (whose elements are of finite order) corresponds to under this embedding.

32. Determine which of the following groups are solvable and/or nilpotent.

(i) The alternating groups  $A_n$  for  $n \geq 3$ .

(ii) The symmetric groups  $S_n$  for  $n \geq 2$ .

(iii) The dihedral groups  $D_n$  for  $n \geq 4$ . (Hint: what is the center of  $D_n$ ?)

(iv) The group of upper unitriangular  $n$  times  $n$  matrices over a field  $F$ .

(v) The group of invertible upper triangular  $n \times n$  matrices over a field  $F$ .

(vi) A group of order  $pq$  where  $p \neq q$  are primes.

(i) For  $n \geq 5$  they are non-abelian simple groups so neither solvable nor nilpotent. For  $n = 3$  its abelian so both solvable and nilpotent. For  $n = 4$ , the center of  $A_4$  is the union of the conjugacy classes of size 1, so it is trivial. Hence it cannot be nilpotent. But it is solvable –  $A_4 > V_4 > C_2 > 1$  is a composition series and all the comp factors are cyclic of prime order.

(ii)  $S_2$  is both,  $S_3 = D_3$  is solvable but not nilpotent,  $S_4$  is solvable but not nilpotent. All others are neither solvable nor nilpotent because  $A_n$  is a subgroup.

(iii) If  $n$  is a power of 2 then  $D_n$  is a 2-group so its both solvable and nilpotent. Otherwise if  $n$  is odd then  $Z(D_n) = 1$  so its not nilpotent; if  $n$  is even then  $D_{n/2}$  is a quotient of  $D_n$  so by induction you get that  $D_n$  is not nilpotent. But of course all  $D_n$  are solvable since  $C_n < D_n$  and  $C_n$  is abelian.

(iv) This is nilpotent, hence solvable. The commutator subgroup is all guys with zeros one diagonal above the main diagonal. The next term in the descending central series is all guys with zeros two diagonals above the main diagonal. Etc...

(v) This is not nilpotent. The commutator subgroup is all upper unitriangular matrices. But  $[G, G'] = G'$  again. But it is solvable, since it is a semidirect product of  $G'$  (which is nilpotent) by the diagonal matrices (which is abelian).

Actually I lied a little here when I wrote that  $[G, G'] = G'$ . If  $n = 1$  then it is nilpotent. And if  $F$  is the field  $\mathbb{Z}_2$  with 2 elements then this is the same group as in (iv) so it is nilpotent. But in all other cases it is not nilpotent.

To prove it is not nilpotent in general, it is enough to focus on  $2 \times 2$  matrices over  $F$  since that is a subgroup of all bigger matrices. Here just compute by brute force to see that if  $|F| > 2$  then  $[G, G'] = G'$  as I said so it is not nilpotent...

(vi) Remember the classification of such groups. WLOG  $p > q$ . If  $q \nmid p - 1$  then its abelian, hence both solvable and nilpotent. If  $q \mid p - 1$  its either abelian, hence both solvable and nilpotent, or else its a non-abelian semidirect product  $C_p \rtimes C_q$ . In that case its solvable but not nilpotent: the center is trivial...

33. True or false? If true give a proof, if false give a counterexample...

(i) If  $G$  is a finite nilpotent group, and  $m$  is a positive integer dividing  $|G|$ , then there exists a subgroup of  $G$  of order  $m$ .

(ii) If  $N$  is a normal subgroup of  $G$  and  $N$  and  $G/N$  are nilpotent, then  $G$  is nilpotent.

(iii)  $S_4/V_4 \cong S_3$ .

(iv) Let  $G$  be a finite group. Then  $G$  is nilpotent if and only if  $N_G(H) \not\leq H$  whenever  $H \leq G$ .

(v) The group  $(\mathbb{Q}, +)$  has a proper subgroup of finite index.

(i) TRUE. Recall that  $G$  is the direct product of its Sylow  $p$ -subgroups. So it suffices to prove the statement for  $p$ -groups. But then its definitely true (a  $p$ -group has a subgroup of every prime order dividing the order of the group...)

(ii) FALSE. For example  $D_5$  is not nilpotent. But it is an extension of  $C_5$  by  $C_2$  which are both nilpotent...

(iii) TRUE. The quotient is non-abelian. Hence its  $S_3$  since that's the only non-abelian group of order 6.

(iv) TRUE. If  $G$  is nilpotent, it's the product of its Sylow  $p$ -subgroups and there is a unique one for each prime. So the subgroups of  $G$  are all direct products of subgroups of these Sylow  $p$ -subgroups. Hence it suffices to prove this for a finite  $p$ -group. See the lemma just before we proved the Sylow theorems...

For the converse, suppose that  $G$  is not nilpotent. Then for some prime  $p$ ,  $G$  has more than one Sylow  $p$ -subgroup. Let  $P$  be one such Sylow  $p$ -subgroup. Then  $N_G(P) \neq G$  (since the index  $[G : N_G(P)]$  is the number of Sylow  $p$ -subgroups). I now claim that  $N_G(N_G(P)) = N_G(P)$  which completes the proof...

To prove the claim suppose that  $g \in G$  normalizes  $N_G(P)$ . Then since  $P$  is the unique Sylow  $p$ -subgroup of  $N_G(P)$  it follows that  $g$  normalizes  $P$ . Hence  $g \in N_G(P)$ .

(v) FALSE. Let  $H$  be a proper subgroup. First note that there is some  $a \in \mathbb{Q} \setminus H$  and some prime  $p$  such that  $pa \in H$ . Indeed, note that  $H \cap \mathbb{Z}$  contains a positive number, say,  $z$ . Now, take any  $a' \in \mathbb{Q} \setminus H$  and multiply it by various primes to make it an integer divisible by  $z$ . Then the product will certainly belong to  $H$ . Now undo the process step by step until you get out of  $H$ .

Now, let us take  $a$  and  $p$  as in the previous paragraph. We claim that  $a, a/p, a/p^2, \dots$  all belong to different  $H$  cosets. Otherwise:  $a/p^n = a/p^k + h$  for some  $n > k$  and  $h \in H$ , whence  $a = p^{n-k}a + p^k h \in H$ , contradiction.

34. Let  $G$  be a finite group.

(i) Prove that if  $G$  is solvable, then  $G$  contains a non-trivial normal abelian subgroup.

(ii) Prove that if  $G$  is not solvable then it contains a normal subgroup  $H$  such that  $H' = H$ .

(i) Each term in the derived series is normal in  $G$ . Take the last non-trivial term in the derived series. Its non-trivial, normal and abelian.

(ii) Since  $G$  is finite and not solvable, the derived series must eventually stabilize at some  $H$  such that  $H' = H$ . But then  $H$  is normal in  $G$  since each term in the derived series is normal in  $G$ .

35. Compute the order of the group  $\langle a, b, c, d \mid bab^{-1} = a^2, bdb^{-1} = d^2, c^{-1}ac = b^2, dcd^{-1} = c^2, bd = db \rangle$ .

2. Just chase the relations around a bit...

36. Suppose that  $X$  is a subset of  $Y$ . Let  $F(X)$  be the free group on  $X$  and  $F(Y)$  be the free group on  $Y$ . Using universal properties, prove that the inclusion  $X \hookrightarrow Y$  induces an injective homomorphism  $F(X) \hookrightarrow F(Y)$ .

By the universal property of  $F(X)$ , there is a homomorphism  $F(X) \rightarrow F(Y)$  such that  $x \mapsto x$  for each  $x \in X$ . This gives an epimorphism from  $F(X)$  to the subgroup of  $F(Y)$  generated by  $X$ . The problem is to prove that this map is injective.

Let  $G$  be the subgroup of  $F(Y)$  generated by  $X$  and let  $i : X \rightarrow G$  be the inclusion of  $X$  into  $G$ . I'll prove that  $(G, i)$  satisfies the universal property to be the free group on  $X$ . This implies that the map constructed in the previous paragraph is actually an isomorphism and we're done.

Take any group  $H$  and a set map  $f : X \rightarrow H$ . Extend  $f$  to  $f' : Y \rightarrow H$  such that  $f'(x) = f(x)$  for all  $x \in X$  and  $f'(y) = 1$  for all  $y \in Y - X$ . By the universal property of  $F(Y)$  there is a unique  $\bar{f}' : F(Y) \rightarrow H$  extending  $f'$ . Now let  $\bar{f}$  be its restriction to  $G$ . This gives a homomorphism  $\bar{f} : G \rightarrow H$  extending  $f$  as required, and it's clearly unique as  $X$  generates  $G$ . We're done.

37. Prove that the group with presentation  $\langle a, b \mid a^6 = 1, b^2 = a^3 = (ab)^2 \rangle$  is of order 12.

It is easy using the relations to see that this group, call it  $G$ , has elements  $a^i b^j$  for  $0 \leq i < 6, 0 \leq j < 2$ . Hence  $|G| \leq 12$ . Now we need a concrete realization...

Consider the subgroup  $K$  of  $\mathbb{H}^\times$  generated by  $e^{2\pi i/6}$  and  $j$ . Note these satisfy the same relations as  $a$  and  $b$ . So there is an epimorphism  $G \rightarrow K$  sending  $a$  to  $e^{2\pi i/6}$  and  $b$  to  $j$ . But it's easy to see  $K$  is of order 12. Hence  $|G| \geq 12$ .

Note this is a presentation for the group of order 12 that we have been calling  $T$ ...

38. The goal of this problem is to derive a presentation for the symmetric group  $S_n$ . Let  $G_n$  be the group with generators  $\{s_1, s_2, \dots, s_{n-1}\}$  subject to the relations  $s_i^2 = 1, s_i s_j = s_j s_i$  for  $|i - j| > 1$  and  $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ . Let  $S_n$  denote the symmetric group, and  $t_i$  denote the basic transposition  $(i \ i + 1)$  in  $S_n$ .

(i) Prove that the  $t_i$  satisfy the same relations as the  $s_i$ .

(ii) Embed  $S_{n-1}$  into  $S_n$  as the subgroup consisting of all permutations fixing  $n$ . Prove that  $\{1, t_{n-1}, t_{n-2}t_{n-1}, \dots, t_1 t_2 \dots t_{n-1}\}$  is a set of  $S_n/S_{n-1}$ -coset representatives.

(iii) By considering the subgroup  $G_{n-1}$  of  $G_n$  generated by  $s_1, \dots, s_{n-2}$  only and using induction, prove that  $G_n \cong S_n$ .

(i) They do.

(ii) Consider the orbit map  $S_n \rightarrow \{1, \dots, n\}, g \mapsto gn$ . The stabilizer of  $n$  is  $S_{n-1}$ . Hence the orbit map induces a bijection  $S_n/S_{n-1} \rightarrow \{1, \dots, n\}$ . Since  $1, t_{n-1}, t_{n-2}t_{n-1}, \dots, t_1 t_2 \dots t_{n-1}$  map  $n$  to  $n, n-1, n-2, \dots, 1$  respectively, they all belong to different cosets. Hence since there are the right number of them they form a system of coset representatives.

(iii) By the universal property, there is a homomorphism  $G_n \rightarrow S_n, s_i \mapsto t_i$ . It is onto since the  $t_i$ 's generate  $S_n$  (midterm!). Now to show it is an isomorphism we just need to prove that  $|G| \leq n!$ . I'll do this by induction on  $n$ .

Consider  $G_{n-1}$ , the subgroup of  $G_n$  generated by  $s_1, \dots, s_{n-2}$ . Note  $G_{n-1}$  is a quotient of the group on generators  $s'_1, \dots, s'_{n-2}$  subject to the same relations. Hence by induction  $|G_{n-1}| \leq (n-1)!$ . Therefore we will be done if we can show that

$$G_n = G_{n-1} \cup s_{n-1}G_{n-1} \cup s_{n-2}s_{n-1}G_{n-1} \cup \dots \cup s_1 \dots s_{n-1}G_{n-1}.$$

To prove this, it suffices to check that the right hand side of this equation is invariant under left multiplication by any  $g \in G$ . Indeed since  $G$  is generated by the  $s_i$  it is enough to see that the right hand side is invariant under left multiplication by any  $s_i$ . So consider

$$s_i s_j s_{j+1} \dots s_{n-1} G_{n-1}.$$

If  $i \leq j$  it is clear enough that this is contained in the right hand side. So assume  $i > j$ . Then you commute the  $s_i$  to the right until you get  $s_i s_{i-1} s_i$ . This equals  $s_{i-1} s_i s_{i-1}$ . Now the rightmost  $s_{i-1}$  commutes to the right until it gets swallowed up by  $G_{n-1}$ . We're done.

39. Let  $G$  and  $H$  be groups. Suppose that  $G$  has the presentation  $G = \langle X | R \rangle$  and  $H$  has the presentation  $H = \langle Y | S \rangle$ . (Why does any group have at least one presentation?). The *free product*  $G * H$  is the group with generators  $X \sqcup Y$  (disjoint union) subject to the relations  $R \sqcup S$ .

(i) There are obvious maps  $G \rightarrow G * H$  and  $H \rightarrow G * H$ . Construct them.

(ii) Prove that  $G * H$  together with these maps is a coproduct of  $G$  and  $H$  in the category of groups.

(iii) Deduce that the group  $G * H$  is independent of the presentations of  $G$  and  $H$  chosen (up to canonical isomorphism).

(iv) Consider the matrices

$$A = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

in  $GL_2(\mathbb{C})$ . Prove that  $A^2 = B^2 = 1$  but that  $AB$  has infinite order.

(v) Deduce that the subgroup of  $GL_2(\mathbb{C})$  generated by the matrices  $A$  and  $B$  is isomorphic to the free product  $C_2 * C_2$ .

(i) in  $G * H$  the elements  $X$  satisfy the relations  $R$ . Hence by the universal property of  $\langle X | R \rangle$  there's a homomorphism  $G \rightarrow G * H$  sending elements of  $X$  to their canonical image. Similarly for  $H$ .

(ii) Take another group  $C$  with maps  $G \rightarrow C$  and  $H \rightarrow C$ . The relations  $R$  and  $S$  are then satisfied in  $C$ . Hence by the universal property of  $\langle X \sqcup Y \mid R \sqcup S \rangle$  there is a map from  $G * H$  to  $C$ ...

(iii) Yes its the coproduct, coproducts are unique up to canonical isomorphism

(iv) You have to compute  $(AB)^n$  for arbitrary  $n$ . It is not too bad... do the first two or three and you'll see the general pattern. Clearly it never repeats 'cos things are always getting bigger.

(v)  $C_2 * C_2$  is the group  $\langle a, b \mid a^2 = b^2 = 1 \rangle$ . So by (iv) there is a map from  $C_2 * C_2$  to  $GL_2(\mathbb{C})$ ,  $a \mapsto A, b \mapsto B$ . The problem is to show that this map is injective.

Clearly every element in  $C_2 * C_2$  can be written either as  $abababab...$  or as  $babababab...$ . We just need to observe all the corresponding matrices are distinct in  $GL_2(\mathbb{C})$ . That is easy enough to do given (iv).

40. Since I know you love the word "unitriangular". Let  $q$  be a power of a prime  $p$ .

(i) Prove that the upper unitriangular matrices are a Sylow  $p$ -subgroup of the group  $GL_n(\mathbb{F}_q)$ .

(ii) How many different Sylow  $p$ -subgroups are there in  $GL_n(\mathbb{F}_q)$ ?

(i) Recall

$$|GL_n(q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

Also

$$|U_n(q)| = q^{n(n-1)/2}.$$

The quotient is  $(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$  which is not zero modulo  $p$ . So it is a Sylow  $p$ -subgroup.

(ii) The normalizer of  $U_n(q)$  is the group  $B_n(q)$  of all upper triangular invertible matrices. To prove this you observe that  $B_n(q)$  is obviously contained in the normalizer of  $U_n(q)$ . Now you use the decomposition

$$GL_n(q) = \bigcup_{w \in S_n} B_n(q)wB_n(q)$$

where  $S_n$  is viewed as the subgroup of  $GL_n(q)$  consisting of all *permutation matrices*. This equation follows by thinking about row and column operations implemented by left and right multiplication by upper triangular matrices. Now take  $g$  in the normalizer of  $U_n(q)$  that does not lie in  $B_n(q)$ . Then  $g = b_1wb_2$  for  $b_1, b_2 \in B_n(q)$  and  $1 \neq w \in S_n$ . Hence  $w$  also lies in the normalizer. But it is obvious that a non-identity permutation matrix doesn't normalize  $U_n(q)$ ... it permutes rows and columns so messes up unitriangularity.

The number of conjugates of  $U_n(q)$  in  $GL_n(q)$  is of course the *index of its normalizer*. (Why? This is the thing to remember from this problem.) So it is  $[GL_n(q) : B_n(q)]$  which is

$$\frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})}{q^{n(n-1)/2}(q - 1)^n}.$$

This simplifies to

$$1(q + 1)(q^2 + q + 1) \cdots (q^{n-1} + \cdots + q^2 + q + 1).$$

If I write

$$[n]_q := q^{n-1} + \cdots + q^2 + q + 1$$

(often called a *Gaussian integer*) and then set

$$[n]_q! := [n]_q [n-1]_q \cdots [2]_q [1]_q$$

then we've shown that  $GL_n(q)$  has  $[n]_q!$  different Sylow  $p$ -subgroups. This is the Gaussian factorial...