

1 Homework 1.

1. (Algebraic independence) Suppose G_1 and G_2 are two groups. We say G_1 and G_2 are *algebraically independent* if there are no proper normal subgroups N_1 and N_2 of G_1 and G_2 , respectively, such that $G_1/N_1 \simeq G_2/N_2$.
 - (a) Prove that G_1 and G_2 are algebraically independent if and only if $G_1 \times G_2$ satisfies the following property: suppose H is a subgroup of $G_1 \times G_2$ and the projection of H to i -th component is G_i for $i = 1, 2$. Then $H = G_1 \times G_2$.
 - (b) Suppose G_1 and G_2 are two finite groups and $\gcd(|G_1|, |G_2|) = 1$. Prove that G_1 and G_2 are algebraically independent.

(**Hint.** Given group homomorphisms $f_i : G_i \rightarrow K$, let

$$G_1 \times_K G_2 := \{(x_1, x_2) \in G_1 \times G_2 \mid f_1(x_1) = f_2(x_2)\}.$$

Note that $G_1 \times_K G_2$ is a subgroup of $G_1 \times G_2$ and the following is a commuting diagram

$$\begin{array}{ccc} G_1 \times_K G_2 & \xrightarrow{\text{pr}_1} & G_1 \\ \text{pr}_2 \downarrow & & \downarrow f_1 \\ G_2 & \xrightarrow{f_2} & K \end{array}$$

(Observe that for every group homomorphism $p_i : L \rightarrow G_i$ such that the following is a commuting diagram, then there exists a unique group homomorphism $f : L \rightarrow G_1 \times_K G_2$ such that the diagram commutes

$$\begin{array}{ccccc} L & & & & \\ & \searrow f & & \searrow p_1 & \\ & G_1 \times_K G_2 & \xrightarrow{\text{pr}_1} & G_1 & \\ & \text{pr}_2 \downarrow & & \downarrow f_1 & \\ & G_2 & \xrightarrow{f_2} & K & \\ & \nearrow p_2 & & \nearrow & \end{array}$$

Simply, consider $f(l) := (p_1(l), p_2(l))$. This group is called *the fiber product of G_1 and G_2 over K* .)

Show that if f_1 is surjective, then pr_2 is surjective, and similarly, if f_2 is surjective, then pr_1 is surjective.

(Argue why $\ker \text{pr}_2 = \ker f_1 \times \{1\}$ and $\ker \text{pr}_1 = \{1\} \times \ker f_2$.)

Next, we want to show if H is a subgroup of $G_1 \times G_2$ and $\text{pr}_i : H \rightarrow G_i$ is surjective for $i = 1, 2$, then $H = G_1 \times_K G_2$ for some surjective $f_i : G_i \rightarrow K$.

Assuming this is the case, $K \simeq G_1 / \ker f_1$ and $\ker \text{pr}_2 = \ker f_1 \times \{1\}$. Therefore, to find out what $\ker f_1$ is, we must consider

$$N_1 := \text{pr}_1(\ker \text{pr}_2) = \text{pr}_1(H \cap (G_1 \times \{1\})).$$

Similarly, we must consider

$$N_2 := \text{pr}_2(\ker \text{pr}_1) = \text{pr}_2(H \cap (\{1\} \times G_2)).$$

Use surjectivity of pr_i 's to show N_j is a normal subgroup of G_j . In particular, $N_1 \times N_2$ is a normal subgroup of H . Prove that projection to the i -th component induces an isomorphism $p_i : H/(N_1 \times N_2) \rightarrow G_i/N_i$. Let $K := H/(N_1 \times N_2)$ and define

$$f_i : G_i \rightarrow K, \quad f_i(g_i) := p_i^{-1}(g_i N_i).$$

Prove that $H = G_1 \times_K G_2$.

(The last part can be done more concretely as well.))

2. Suppose G is a finite group. Suppose for every positive integer n ,

$$|\{g \in G \mid g^n = e\}| \leq n,$$

where e is the neutral element of G . Use the following steps to prove that G is a cyclic group.

- (a) Prove that if there is an element of order d in G , then there are exactly $\phi(d)$ elements of order d in G , where $\phi(d)$ is the Euler ϕ -function.
- (b) For every positive number d , let $\psi(d)$ be the number of elements of G that has order d . Show that $\psi(d) \leq \phi(d)$ and $\psi(d) \neq 0$ implies that $d \mid |G|$.
- (c) Prove that $\psi(d) = \phi(d)$ if d is a positive divisor of $|G|$. Deduce that G is a cyclic group. (Hint. Use the previous step and the fact that $\sum_{d \mid n} \phi(d) = n$ for every positive integer n .)

(Remark. Later we will use this result to deduce that the group of units of every finite field is cyclic.)

- Find the automorphism group of the Cayley graph of $\mathbb{Z}$ with respect to the set $S := \{1, -1\}$. (You have to list the elements of this group, and write the product of every two elements as an element in the given list.)
- (Symmetries and Diophantine equations) Suppose a and b are non-negative integers. Prove that if $k = \frac{a^2+b^2}{1+ab}$ is an integer, then k is a perfect square.

(Hint. We look for some symmetries of the set

$$V := \{(a, b) \in \mathbb{Z}^2 \mid a^2 + b^2 - kab - k = 0\}.$$

View this equation as a quadratic equation in terms of a . Deduce that the sum of two zeros is kb . Thus if $(a, b) \in V$, then $(b, kb - a) \in V$. Hence, multiplication by the matrix $\begin{pmatrix} 0 & 1 \\ -1 & k \end{pmatrix}$ is a *symmetry* of V . Argue that you may assume $k \geq 2$, and $(a, b) \in V$ implies $a \neq b$ and $\text{sgn}(a)\text{sgn}(b) \geq 0$. Deduce that if $(a, b) \in V$ and $a > b > 0$, then $kb - a \geq 0$. Argue why $b > kb - a$. Deduce that if $(a_0, b_0) \in V$, $a_0 > b_0 \geq 0$ and a_0 is smallest such integer, then $b_0 = 0$. Thus, $k = a_0^2$.

Can you use this argument to list all the elements of V ?

(Remark. The idea of using symmetries of an equation in order to find many solutions is extremely useful. An important example is the Markoff equation

$$x^2 + y^2 + z^2 = 3xyz.$$

Clearly $(1, 1, 1)$ is a solution of the Markoff equation. Using a similar argument as the above problem, we get that if (a, b, c) is a solution of the Markoff equation, then so are $(3bc - a, b, c)$, $(a, 3ac - b, c)$, and $(a, b, 3ab - c)$. Moreover, we can permute the components and change the sign of two of the components. It turns out starting with $(1, 1, 1)$ using the above mentioned symmetries, one can get all the integer solutions of the Markoff equation.)

- Recall that an automorphism of a group G is a group isomorphism from G to itself. The set of all the automorphisms of G is denoted by $\text{Aut}(G)$. One can see that $\text{Aut}(G)$ forms a group under the composition of functions. In

this problem, we want to prove that $\text{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, where C_n is a cyclic group of order n and $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements of $\mathbb{Z}/n\mathbb{Z}$ that have multiplicative inverse.

- (a) Suppose $C_n = \langle g \rangle$ and $\phi \in \text{Aut}(C_n)$. Suppose $\phi(g) = g^m$. Prove that $\gcd(m, n) = 1$. (Hint. Use the fact that $o(g) = o(\phi(g))$ and $o(g^m) = \frac{o(g)}{\gcd(o(g), m)}$.)
- (b) Suppose $\gcd(m, n) = 1$. Prove that $\phi_m : C_n \rightarrow C_n, \phi_m(x) := x^m$ is an automorphism of C_n .
- (c) Prove that $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(C_n), (m + n\mathbb{Z}) \mapsto \phi_m$ is an isomorphism.