Random Algebra/Number Theory Problems

Shaun Ostoic

June 7, 2018

Exercise 1. Let G be a finite group. Show that $a \in G$ is a generator of G if and only if $a^{\frac{|G|}{q}} \neq 1$, for each prime factor p of $|G|$.

Proof. $(\rightarrow)$ Since a generates G, it is a cyclic group, hence $G = \langle a \rangle$. A consequence of this is that $|G| = |\langle a \rangle| = |a|$. Let us assume for sake of a contradiction, that $a^{\frac{|G|}{q}} = 1$ for some prime factor q of $|G|$. Then we see that $a^{\frac{|G|}{q}} = 1 \implies |a| \text{ divides } \frac{|G|}{q} \implies |a| = |G| < \frac{|G|}{q}$, which is a contradiction.

$(\leftarrow)$ Assume $a^{\frac{|G|}{q}} = 1$ for every prime factor q of $|G|$. Since $\langle a \rangle$ is a subgroup of G, $|\langle a \rangle| \text{ divides } |G|$ (by Lagrange's Theorem. Let $m = \frac{|G|}{q}$. Then

$$|a^m| = \frac{|a|}{(m, |a|)}.$$

We claim that $|a^m| = q$. To see this, observe that

$$(a^{\frac{|G|}{q}})^q = a^{|G|} = 1.$$

From this we see that $|a^m| \text{ divides } q$. Since $a^m \neq 1$ and q is prime, it follows that $|a^m| = q$. Thus,

$$|a^m| = \frac{|a|}{(m, |a|)} = q$$

$$|a| = q(m, |a|)$$

$$\implies q \text{ divides } |a|.$$

Since q was an arbitrary prime factor of $|G|$, we see that every prime factor of $|G| \text{ divides } |a|$. $\square$