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.

($\Leftarrow$) Suppose instead that a is not a generator of G. Then $|a| \neq |G|$, which means there must be a prime divisor q of $|G|$ for which $|a| \ \text{divides} \ \frac{|G|}{q}$. To be more explicit, let us look at the prime factorization of $|G|$ and of $|a|$. Write $|G| = q_1^{g_1} \dots q_r^{g_r}$ and $|a| = q_1^{a_1} \dots q_r^{a_r}$, with $a_i \leq g_i$ for all i. It is entirely possible that a may hold each prime divsior of $|G|$ in its prime factorization, but it does not necessarily have equal exponents in the factorization. Otherwise, $a_i = g_i$ for all i, hence $|a| = |G|$. In this case, $|a|$ and $|G|$ must differ by at least one prime divisor q. Then if we divide out that prime factor from $|G|$, it follows that $|a| \ \text{divides} \ \frac{|G|}{q}$. By one of the previous theorems, this is equivalent to saying that $a^{\frac{|G|}{q}} = 1$, which contradicts the assumption we make in this direction of the proof.

$\square$

Exercise 2. Show that for any prime number $p \geq 3$, $\mathbb{Z}_p^*$ has a primitive root.

Proof. To show that $\mathbb{Z}_p^*$ has a primitive root, it is sufficient to show that $|a| = \phi(p) = p - 1$, for some $a \in \mathbb{Z}_p^*$. $\square$

Exercise 3. Show that a finite subset B of a vector space V over a field F is a basis for V if and only if every $v \in V$ can be written uniquely as a linear combination of vectors from B. That is, where $B = \{b_1, \dots b_n\}$, the scalars $\alpha_i \in F$ for all i are unique for which

$$v = \alpha_1 b_1 + \ldots + \alpha_n b_n.$$

Proof. ($\Rightarrow$) Suppose that B is a basis for V. Then B is both a spanning set, and a linearly independent set. It is a spanning set for V, which means that for every $v \in V$, there exist scalars $\alpha_1, \dots \alpha_n \in F$ such that

$$v = \alpha_1 b_1 + \cdots + \alpha_n b_n. \tag{1}$$

B being linearly independent means that if there exist $\eta_1, \dots \eta_n \in F$ such that

$$\eta_1 b_1 + \cdots + \eta_n b_n = 0,$$

then $\eta_i = 0$ for all i.

We must now show that (1) is the only possible way to write v as a linear combination of vectors from B. Suppose for sake of a contradiction that there is another such way to write v, that being

$$v = \beta_1 b_1 + \cdots + \beta_n b_n, \tag{2}$$

where $\beta_1, \ldots \beta_n \in F$. Using (1) and (2), we have

$$\beta_1 b_1 + \cdots + \beta_n b_n = \alpha_1 b_1 + \cdots + \alpha_n b_n$$

$$(\alpha_1 - \beta_1) b_1 + \cdots + (\alpha_n - \beta_n) b_n = 0 \tag{3}$$

Let us use the assumption that B is a linearly independent set. Set $\eta_i = (\alpha_i - \beta_i)$ for each i. Then (3) can be written as

$$\eta_1 b_1 + \cdots + \eta_n b_n = 0,$$

which implies that $\eta_i = 0$ for all i by linear indepdendence of B. That is, $\alpha_i - \beta_i = 0$, hence $\alpha_i = \beta_i$ for all i, which proves that these two ways of writing v are the same.

($\Leftarrow$) Suppose that $\square$

Exercise 4. content...