Math 113 — Problem Set 6 — William Guss

(P67. 41) Find the primitive roots of U_{12}.

Proof. We claim that $\{exp(i1 \times 2\pi/12), exp(i5 \times 2\pi/12), exp(i7 \times 2\pi/12, exp(i11 \times 2\pi/12)\}$ are the primitive roots of U_{12}. First observe that $\{1, 2, 3, 4, 6, 12\}$ all divide 12 and there is an isomorphism between $\mathbb{Z}_{12}$ and U_{12} so that the strict subgroups generated by each of those integers do not isomorphically describe the full group U_{12}, again using the same isomorphism argument, any multiple of those numbers (by themselves) are just a part of the same subgroup and themselves generate potentially a smaller subgroup then those subgroups. Therefore we look for elements in $\mathbb{Z}_{12}$ which are not multiples of the divisors of 12 but are less than 12 (except for 1). We get $1, 5, 7, 11$. Therefore using the cannonical isomorphism we get the claimed set of primitive roots. □

(83. 2) We compute the permutation.

Proof. (I need to use a *Solution.* environment.) First

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$$

so we get therefore

$$\tau^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \\ 1 & 2 & 3 & 6 & 5 & 4 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}$$

□

(84. 16) Find the number of elements in the set $\{\sigma \in S_4 \mid \sigma(3) = 3\}$.

Proof. Any permutation is permitted as long as $\sigma(3) = 3$. Therefore we accept 3 choices and restrict the first. Therefore there must be $3 \times 2 \times 1 = 6$ permutations. □

(84. 30) Show that $f_1 : \mathbb{R} \to \mathbb{R}$ such that $f_1(x) = x + 1$ is a bijection (and therefore a permutation.)

Proof. First for every $x \in \mathbb{R}$ there exists a unique sucessor, nameley $x + 1$, by the archimedian property. Therefore we have an injection. Furthermore $x + 1 = y$ if and only if $y - 1 = x$ since $\mathbb{R}$ is an Abelian group on addition. Thus $f_1 : x \mapsto x + 1$ is a bijection. □

(84. 31) Show that $f_2 : \mathbb{R} \to \mathbb{R}$ such that $f_2(x) = x^2$ is not bijection (and therefore not permutation.)

Proof. First observe that $x^2 = 1$ is $x = -1$ OR if $x = 1$. Therefore the mapping is not injective. Therefore the map is not a bijection. □

(84. 32) Show that $f_3 : \mathbb{R} \to \mathbb{R}$ such that $f_3(x) = -x^3$ is a bijection (and therefore a permutation.)

Proof. Clearly $-(\cdot)$ is a permutation and the composition of permutations is a permutation by the definition. We now show that x^3 is a permutation. First if $x \neq y$ then without loss of generality $x > y$. Furthermore by the montonicty of $x \mapsto x^3$ (basic calculus) we have that $x^3 > y^3 \iff x^3 \neq y^3$ by the well ordering of $\mathbb{R}$. Finally take any $z \in \mathbb{R}$. We claim that there is an x say $x = \sqrt[3]{z}$ so that $x^3 = z$. First by the completeness of $\mathbb{R}$ and the cauchy approximation sequence of $\sqrt[3]{z}$ in $\mathbb{Q}$ we have the existence of x. Finally $x^3 = z^{1/3\times 3} = z$. Therefore the map is a surjection. This completes the proof. $\square$