Graduate Algebra
Homework 3 Solutions

Fall 2014

Due 2014-09-17 at the beginning of class

1. (a) Show that $\mathrm{Aut}(\mathbb{Q}) \cong \mathbb{Q}^\times$.
   (b) Show that $\mathrm{Aut}(\mathbb{R}) \supsetneq \mathbb{R}^\times$. [Hint: Take a suitable $\mathbb{Q}$-vector space projection from $\mathbb{R}$ to $\mathbb{Q}$.]
   (c) (Extra credit) Find all groups G such that $\mathrm{Aut}(G) = \{\mathrm{id}\}$. [This is a fun exercise.]

   Proof. (a): If $f \in \mathrm{Aut}(\mathbb{Q})$ then $f(nx) = nf(x)$ for all x. In particular $f(n) = nf(1)$ and $f(m) = nf(m/n)$ so $f(m/n) = f(1) \cdot m/n$. Thus all automorphisms are given by multiplication by $f(1)$ and this is invertible iff $f(1) \neq 0$.

   (b): Again $\mathbb{R}^\times \subset \mathrm{Aut}(\mathbb{R})$ because if $r \neq 0$ then $f(x) = rx$ is an automorphism. How to get more automorphisms? $\mathbb{R}$ is a vector space over $\mathbb{Q}$ so fix some basis $\mathcal{B} = \{a, b, c, \ldots\}$ (uncountable, but choose a, b, c basis vectors). Every $r \in \mathbb{R}$ is a finite linear combination of basis vectors with $\mathbb{Q}$-coefficients. So $r = r_a a + r_b b + r_c c + \cdots$. Consider $f(r) = r_b a + r_a b + r_c c + \cdots$ (swap the coefficients of a and b). Then this is a homomorphism of groups (coefficients are additive since every linear combination of basis vectors is unique). But $f(c) = c$ so if f were multiplication by a real number it would have to be the identity map. However $f(a) = b$ so f is not multiplication by any real number.

   (c): $\mathrm{Inn}(G) = 1$ so $gxg^{-1} = x$ for all g, x so G is abelian. Since G is abelian, $x \mapsto x^{-1}$ is a homomorphism so $x^{-1} = x$ for all x, thus $x^2 = 1$ for all x. This implies that G is a vector space over $\mathbb{F}_2$, scalar multiplication being given by $c \cdot x = x^c$, which is well-defined since $x^2 = 1$. Let $\mathcal{B}$ be a basis of G over $\mathbb{F}_2$. If $\dim \mathcal{B} > 1$, the "swapping of coefficients" argument from (b) shows that there exists a nontrivial automorphism. Thus $\dim \mathcal{B} \leq 1$ and so $G = 1$ or $G = \mathbb{Z}/2\mathbb{Z}$. Both have trivial automorphism groups. ☐

2. Let p be a prime number. Consider $G = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z}\}$.

   (a) Show that G is a group.
   (b) Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and define $H_a = \{\begin{pmatrix} a^k & b \\ 0 & 1 \end{pmatrix} | b \in \mathbb{Z}/p\mathbb{Z}, k \in \mathbb{Z}\}$. Show that H_a is a normal subgroup of G.
   (c) Show that every proper normal subgroup of G is of the form H_a for some a. [Hint: You will need to use that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group.]
   (d) Show that $G \cong \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$ given by the identity map $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

   We'll study this group later as the **Galois group** of the polynomial $X^p - 2$.

   Proof. Write $(a, b) = \begin{pmatrix} a & b \\ & 1 \end{pmatrix}$. (a) Clearly $(a, b)(c, d) = (ac, ad + b)$ and $(a, b)^{-1} = (a^{-1}, -a^{-1}b)$. Thus G is a group.

(b) Check $(x,y)(a^k,b)(x,y)^{-1} = (xa^k, xb+y)(x^{-1}, -x^{-1}y) = (a^k, (1-a^k)y+xb) \in H_a$ so H_a is normal.

(c) Consider $G \to (\mathbb{Z}/p\mathbb{Z})^\times$ sending (a,b) to a. This is a group homomorphism (from the multiplication formulae). Thus if H is a subgroup of G the image of H under this map is also a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. But this group is cyclic and all subgroups of cyclic groups are cyclic (already proved this when you showed that finite subgroups of $\mathbb{C}$ are groups of roots of unity) it follows that for some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, the image of H is $\langle a \rangle$. Thus for each k there exists some b such that $(a^k, b) \in H$. Since H is normal, for all $(x,y) \in G$ we need $(x,y)(a^k,b)(x,y)^{-1} \in H$. Thus $(a^k, (1-a^k)y+xb) \in H$ for all x, y. If $a^k \neq 1$ it follows that $(a^k, c) \in H$ for all c. Finally, $(a^k, x)(a^{-k}, 0) = (1, x)$ so $H_a \subset H$. If $H \neq H_a$ then H must have some element (x,y) with $x \notin \langle a \rangle$ contradicting the choice of a.

(d): $N = H_1$ is normal and $H = \{(x,0)\}$ is a disjoint subgroup such that $G = NH$. Thus $G \cong N \rtimes H$ with $H \mapsto \operatorname{Aut}(N)$ given by $h \mapsto (n \mapsto hnh^{-1})$. $N \cong \mathbb{Z}/p\mathbb{Z}$ identifying $(1,b)$ with b and $H \cong (\mathbb{Z}/p\mathbb{Z})^\times$ identifying $(x,0)$ with x. What is $\phi : H \to \operatorname{Aut}(N)$ under these isomorphisms? $\phi_h(n) = hnh^{-1}$ so $\phi_x(b)$ can be read from $(x,0)(1,b)(x^{-1},0) = (1,bx)$ thus $\phi_x(b) = bx$ and so $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \to \operatorname{Aut}(\mathbb{Z}/p\mathbb{Z})$ sends x to multiplication by x. □

3. Let G be a finite group and let H be a subgroup of G. Denote by S_H the group of permutations of the finite set G/H.
   (a) Show that if $g \in H$ then the map $f_g : G/H \to G/H$ defined by $f_g(xH) = gxH$ is an element of S_H.
   (b) Show that $G \to S_H$ given by $g \mapsto f_g$ is a group homomorphism with kernel $\ker f$ contained in H.
   (c) Suppose that $[G : H] = p$ is the smallest prime divisor of $|G|$. Show that $|G/\ker f| = p$ and deduce that H is normal in G. [This is a generalization of the standard result that every index 2 subgroup is normal.]

Proof. (a): If $f_g(xH) = f_g(yH)$ then $gxH = gyH$ so $xH = yH$ so f_g is a permutation of G/H.

(b): If $g, h \in G$, $f_g \circ f_h = f_{gh}$ so $f : G \to S_H$ is a group homomorphism. If $g \in \ker f$ then $f_g = \mathrm{id}$ so $f_g(H) = H$. Thus $gH = H$ so $g \in H$ and we deduce $\ker f \subset H$.

(c): $G/\ker f \cong \operatorname{Im} f$ which is a subgroup of S_H. By Lagrange $|G/\ker f| \mid |S_H| = p!$. But $|G/\ker f| \mid |G|$ so $|G/\ker f| \mid (p!, |G|) = p$. Thus $\ker f \subset H \subset G$ with $[G : H] = [G : \ker f]$ so $H = \ker f$ which is then normal in G. □

4. Let G be an abelian group. Suppose $g, h \in G$ have finite orders m and n. Show that $\operatorname{ord}(gh) \mid [m,n]$, the least common multiple of m and n.

Proof. $(gh)^{[m,n]} = g^{[m,n]}h^{[m,n]} = 1$ since $m, n \mid [m,n]$. □

5. Let G be a group such that $G/Z(G)$ is cyclic. Show that G is abelian. Does the same conclusion hold if $G/Z(G)$ is only assumed to be abelian?

Proof. Suppose $G/Z(G) = \langle gZ(G) \rangle = \{(gZ(G))^k\} = \{g^kZ(G)\}$. Then $G = \sqcup g^kZ(G)$. Now $g^iug^jv = g^{i+j}uv = g^jvg^iu$ since $u, v \in Z(G)$. Thus G is cyclic.

From homework 2 the Heisenberg group is nonabelian with $G/Z(G)$ abelian not cyclic. □