Solutions to Homework 1

1. (a) Show that the additive group of $\mathbb{Z}_2[x]/x^2$ is isomorphic to the additive group of $\mathbb{Z}_2 \times \mathbb{Z}_2$, although the rings are not isomorphic.
Solution: Define a map $\varphi\colon \mathbb{Z}_2[x]/x^2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$0 \mapsto (0,0) \qquad 1 \mapsto (0,1) \qquad x \mapsto (1,0) \qquad x+1 \mapsto (1,1).$$

This is clearly a bijection, and the verifaction that $\varphi(a+b) = \varphi(a) + \varphi(b)$ is straightforward.

(b) Show that the additive group of $\mathbb{Z}_4$ is not isomorphic to the additive group of $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Solution: Suppose that $\varphi\colon \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ is a homomorphism of additive groups. Recall that for every $r \in \mathbb{Z}_2 \times \mathbb{Z}_2$ we have $r + r = 0$. Thus

$$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 0 = \varphi(0),$$

so φ is not injective, and in particular not an isomorphism.

2. (a) Show that $\mathbb{Z}_5^\times$ is isomorphic to the additive group of $\mathbb{Z}_4$.
Solution: Define a map $\varphi\colon \mathbb{Z}_4 \to \mathbb{Z}_5^\times$ by

$$0 \mapsto 1 \qquad 1 \mapsto 2 \qquad 2 \mapsto 4 \qquad 3 \mapsto 3.$$

This is clearly a bijection, and the verification that $\varphi(a+b) = \varphi(a) \cdot \varphi(b)$ is straightforward. The other possibility is

$$0 \mapsto 1 \qquad 1 \mapsto 3 \qquad 2 \mapsto 4 \qquad 3 \mapsto 2.$$

(b) Show that $\mathbb{Z}_8^\times$ is isomorphic to the additive group of $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Solution: Define a map $\varphi\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_8^\times$ by

$$(0,0) \mapsto 1 \qquad (1,0) \mapsto 3 \qquad (0,1) \mapsto 5 \qquad (1,1) \mapsto 7.$$

This is clearly a bijection, and the verification that $\varphi(a+b) = \varphi(a) \cdot \varphi(b)$ is straightforward. There are five other possibilities – any permutation of 3, 5, and 7 above works equally well.

(c) Find a some more small numbers n such that $\mathbb{Z}_n^\times$ is isomorphic to the additive group of $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Solution: We have $\mathbb{Z}_4 \cong \mathbb{Z}_{10}^\times$ via the map

$$0 \mapsto 1 \qquad 1 \mapsto 3 \qquad 2 \mapsto 5 \qquad 3 \mapsto 7,$$

and $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_{12}^\times$ via the map

$$(0,0) \mapsto 1 \qquad (1,0) \mapsto 5 \qquad (0,1) \mapsto 7 \qquad (1,1) \mapsto 11.$$

3. Show that $\mathbb{R}^\times$ is isomorphic to (the additive group of) $\mathbb{R} \times \mathbb{Z}_2$.

Solution: Define a map $\varphi\colon \mathbb{R} \times \mathbb{Z}_2 \to \mathbb{R}^\times$ by

$$\varphi(x, a) = e^x \cdot (-1)^a.$$

This is well-defined: if $a \equiv a' \pmod 2$ is even then $(-1)^a = (-1)^{a'}$. It is a homomorphism:

$$\varphi(x + y, a + b) = e^{x+y} \cdot (-1)^{a+b} = e^x(-1)^a e^y(-1)^b = \varphi(x, a) \cdot \varphi(y, b).$$

It is bijective: for $y \in R^\times$, we have

$$\varphi^{-1}(y) = \begin{cases} (\ln|y|, 0) & \text{if } y > 0 \\ (\ln|y|, 1) & \text{if } y < 0. \end{cases}$$

Optional: Show that $\mathbb{Q}^\times$ is not isomorphic to $\mathbb{Q} \times \mathbb{Z}_2$. Can you give a nice description of $\mathbb{Q}^\times$?

Solution: Suppose that there is a homomorphism $\varphi\colon \mathbb{Q} \times \mathbb{Z}_2 \to \mathbb{Q}^\times$. Then $\varphi(0,0) = 1$, and I claim that $\varphi(0,1) = \pm 1$: indeed, if $x = \varphi(0,1)$ then

$$x^2 = \varphi(0,1) \cdot \varphi(0,1) = \varphi(0+0, 1+1) = \varphi(0,0) = 1,$$

so $x = \pm 1$. Next, let $(y, a) = \varphi^{-1}(2)$; then we have

$$\varphi(y, 0) = \varphi(0 + y, a + a) = \varphi(0, a)\varphi(y, a) = \pm 1 \cdot 2.$$

Finally, let $z = \varphi(\frac{1}{2}y, 0)$. Then

$$z^2 = \varphi(\tfrac{1}{2}y + \tfrac{1}{2}y, 0 + 0) = \varphi(y, 0) = \pm 2.$$

But there is no $z \in \mathbb{Q}^\times$ with either $z = 2$ or $z = -2$.

For the nice description, I claim that $\mathbb{Q}^\times$ is isomorphic to the subgroup of the additive group

$$\mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \dots$$

consisting of sequences $(a, n_1, n_2, n_3, \dots)$ for which only finitely many n_i are non-zero. Let p_i be the i^{th} prime, so $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Then the isomorphism to $\mathbb{Q}^\times$ is given by

$$(a, n_1, n_2, n_3, \dots) \mapsto (-1)^a \cdot p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdots .$$

Note that this product is well-defined because only finitely many n_i are non-zero.

4. Find a subgroup of $\mathbb{C}^\times$ that is isomorphic to $\mathbb{Z}_3$.

   Solution: The subgroup is $H = \{1, \omega, \omega^2\}$, where

   $$\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}.$$

   Notice that

   $$\omega^2 = \bar{\omega} = \frac{-1 - \sqrt{-3}}{2}$$

   and $\omega^3 = 1$. The isomorphism $\mathbb{Z}_3 \to H$ is given by $n \mapsto \omega^n$.

5. Recall that $\mathrm{GL}_n(\mathbb{R}) = \mathrm{M}_n(\mathbb{R})^\times$ is the group of invertible $n \times n$ matrices with real entries, under matrix multiplication. Let $\mathrm{GL}_n^+(\mathbb{R})$ denote the subgroup of matrices with positive determinant. Show that if n is odd then $\mathrm{GL}_n \cong \mathrm{GL}_n^+ \times \mathbb{Z}_2$.

   Solution: Define a map $\varphi\colon \mathrm{GL}_n^+ \times \mathbb{Z}_2 \to \mathrm{GL}_n$ by

   $$(A, a) \mapsto (-1)^a \cdot A.$$

   This is well-defined: again, if $a \equiv a' \pmod 2$ then $(-1)^a = (-1)^{a'}$. It is a homomorphism:

   $$\varphi(AB, a+b) = (-1)^{a+b} \cdot AB = (-1)^a \cdot A \cdot (-1)^b \cdot B = \varphi(A, a) \cdot \varphi(B, b).$$

   We have $\det(-A) = (-1)^n \det(A)$, so if n is odd then φ is bijective, with

   $$\varphi^{-1}(A) = \begin{cases} (A, 0) & \text{if } \det A > 0 \\ (-A, 1) & \text{if } \det A < 0. \end{cases}$$

Optional: Show that this is not true if n is even. Hint: Consider the *centers* of the two groups:

$$Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}.$$

Solution: This is a bit fancy.

Claim 1: If G_1 and G_2 are groups then $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$. Proof: For a pair $(g_1, g_2) \in G_1 \times G_2$, the claim is that $g_1 \in Z(G_1)$ and $g_2 \in Z(G_2)$ if and only if $(g_1, g_2) \in Z(G_1 \times G_2)$. This follows from the fact that

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2)$$
$$(h_1, h_2) \cdot (g_1, g_2) = (h_1 g_1, h_2 g_2)$$

for all $h_1 \in G_1$ and $h_2 \in G_2$.

Claim 2: An isomorphism $\varphi\colon G_1 \to G_2$ takes $Z(G_1)$ isomorphically to $Z(G_2)$. Proof: Let $g \in Z(G_1)$; then we will argue that $\varphi(g) \in Z(G_2)$. Indeed, for $h \in G_2$, we have

$$\varphi^{-1}(h) \cdot g = g \cdot \varphi^{-1}(h),$$

because $g \in Z(G_1)$. Taking φ of both sides we get

$$h \cdot \varphi(g) = \varphi(g) \cdot h,$$

so $\varphi(g) \in Z(G_2)$. Similarly, φ^{-1} takes $Z(G_2)$ into $Z(G_1)$.

Claim 3: The center of GL_n is the subgroup of scalar matrices, that is,

$$\begin{pmatrix} x & & \\ & \ddots & \\ & & x \end{pmatrix}$$

for $x \in \mathbb{R}^\times$. Maybe you can say this is well-known, but here's a proof. Clearly the scalar matrices are contained in the center. To prove the reverse inclusion, fix $i \neq j$ between 1 and n, and for $t \in \mathbb{R}$ let M_t be the matrix with 1's down the diagonal and t in the (i, j) entry. Observe that $\det M_t = 1$, so $M_t \in \mathrm{GL}_n^+$. For $A \in Z(\mathrm{GL}_n)$ we have

$$A \cdot M_t = M_t \cdot A.$$

Taking derivatives with respect to t, we find that

$$A \cdot N = N \cdot A,$$

where N is the matrix with 1 in the (i,j) entry and zero elsewhere. Taking the (i,j) entry of both sides we get $a_{ii} = a_{jj}$; taking the (i,i) entry we get $a_{ji} = 0$. Since i and j were arbitrary, we see that all the diagonal entries of A are equal and all the off-diagonal entries are zero, i.e. A is a scalar matrix.

Since $M_t \in \mathrm{GL}_n^+$, the same argument shows that the center of GL_n^+ is the subgroup of scalar matrices

$$\begin{pmatrix} x & & \\ & \ddots & \\ & & x \end{pmatrix}$$

for $x \in \mathbb{R}^\times$ with $x^n > 0$. If n is odd, this means $x > 0$, and if n is even it is no restriction.

Main claim: If n is even then there is no isomorphism

$$\varphi\colon\ \mathrm{GL}_n \to \mathrm{GL}_n^+ \times \mathbb{Z}_2.$$

Proof: In the proof previous claim we saw in fact that if n is even then

$$Z(\mathrm{GL}_n) = Z(\mathrm{GL}_n^+) \cong \mathbb{R}^\times.$$

So taking centers on both sides, we would have an isomorphism

$$\mathbb{R}^\times \to \mathbb{R}^\times \times \mathbb{Z}_2.$$

But in $\mathbb{R}^\times$, there are two elements x with $x^2 = 1$, namely ± 1, and in $\mathbb{R}^\times \times \mathbb{Z}_2$ there are four, namely $(\pm 1, 0)$ and $(\pm 1, 1)$.