Problem	1	2	3	4	5	Total
Grade						

Math 5210 - Abstract Algebra I Final Exam

Rachel Lonchar

Exercise 1. Fix an integer $N > 1$.

(a) Show the matrix group

$$\begin{pmatrix} N^{\mathbb{Z}} & \mathbb{Z}[1/N] \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} N^k & r \\ 0 & 1 \end{pmatrix} : k \in \mathbb{Z}, r \in \mathbb{Z}[1/N] \right\}$$

is generated by the two matrices $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. (Hint: Play around with conjugates of each of these two matrices by the other matrix or its inverse. Write elements of $\mathbb{Z}[1/N]$ as a/N^ℓ with $a \in \mathbb{Z}$ and $\ell \geq 0$. Do *not* use fractional exponents.)

(b) Denote the group in part (a) by H_N. In H_N, $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^N$. Show H_N is "universal for the property $xyx^{-1} = y^N$." That is, if G is any group containing two elements x and y such that $xyx^{-1} = y^N$, show there is a unique group homomorphism $f\colon H_N \to G$ such that $f\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right) = x$ and $f\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = y$. (Hint: From $xyx^{-1} = y^N$, show $x^m y x^{-m} = y^{N^m}$ for $m \geq 0$.)

Solution 1.

(a) For any $k, n, m \in \mathbb{Z}$ with $m \geq 0$, we have $\left(\begin{smallmatrix} N^k & n/N^m \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1/N & n/N^m \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} N^{m+k} & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1/N^m & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} N^{m+k} & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1/N & 0 \\ 0 & 1 \end{smallmatrix}\right)^m\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{m+k} = \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-m}\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{m+k}$. Thus, the group H_N is contained in the group generated by the two matrices $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Since these two matrices are elements of H_N, the group generated by them is obviously contained in H_N and so H_N is the group generated by these two matrices.

(b) If we have $xyx^{-1} = y^N$, then let's assume that $x^{m-1}yx^{-(m-1)} = y^{N^{m-1}}$ for $m \geq 1$, and we shall prove that $x^m y x^{-m} = y^{N^m}$. We have,

$$x^m y x^{-m} = x(x^{m-1}yx^{-(m-1)})x^{-1} = x(y^{N^{m-1}})x^{-1} = (y^{N^{m-1}})^N = y^{N^m},$$

so $x^m y x^{-m} = y^{N^m}$ for $m \geq 0$ by induction.
Since H_N is generated by $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, a mapping defined by the two unique generators will be a unique homorphism. Since G is a group with this property and there is a unique homomorphism of H_N to G, it must be true that H_N is universal for this property as well.

Exercise 2. Let's find all groups of order 2014 up to isomorphism.

(a) Show every group of order 2014 is isomorphic to a semidirect product $\mathbb{Z}/(1007) \rtimes_\varphi \mathbb{Z}/(2)$. (Remember the group law in $\mathbb{Z}/(1007)$ and $\mathbb{Z}/(2)$ is addition, not multiplication!)

(b) Show there are four semidirect products in (a) and they are **non-isomorphic** by checking that the groups have different numbers of elements of order 2.

Solution 2.

(a) Let G be a group of order 2014. The first Sylow theorem states that there are p-Sylow subgroups for each prime p in the group's prime decomposition. Thus, there exists 19-Sylow and 53-Sylow subgroups ($2014 = 2 \cdot 19 \cdot 53$). Also the number of 19-Sylow groups, n_{19} is such that, $n_{19}|53 \cdot 2$ and $n_{19} \equiv 1 \mod 19$ by the Sylow theorems and $53 \equiv 15 \not\equiv 1 \mod 19$, $2 \not\equiv 1 \mod 19$, so $n_{19} = 1$. Similarly, n_{53} is such that, $n_{53}|19 \cdot 2$ and $n_{53} \equiv 1 \mod 53$ by the Sylow theorems and $19 \not\equiv 1 \mod 53$, $2 \not\equiv 1 \mod 53$, so $n_{53} = 1$. Thus, there is a unique 19-Sylow subgroup and a unique 53-Sylow subgroup. Since all p-Sylow subgroups are conjugate, these subgroups must also be normal.

Let P be a subgroup of order 19 and let Q be a subgroup of order 53. We are going to show that the set $PQ = \{xy : x \in P, y \in Q\}$ is a subgroup and $PQ \cong P \times Q \cong \mathbb{Z}/(1007)$. Say $a, b \in PQ$. Then, $a = p_1q_1, b = p_2q_2$ for some $p_1, p_2 \in P, q_1, q_2 \in Q$. Then,

$$ab = p_1q_1p_2q_2 = p_1(q_1p_2q_1^{-1})q_1q_2,$$

where $q_1p_2q_1^{-1} \in P$ since P is normal so that $p_1(q_1p_2q_1^{-1}) \in P$ and $q_1q_2 \in Q$, hence $ab \in PQ$, so that PQ is closed. For inverses, we have $(pq)^{-1} = q^{-1}p^{-1} = (q^{-1}p^{-1}q)q^{-1}$, where $q^{-1}p^{-1}q \in P$ since P is normal, so PQ contains its inverses. Since P and Q are subgroups, they both contain 1 so that $1(1) = 1 \in PQ$ and PQ contains the identity. Thus, PQ is a subgroup.

We have that P and Q are normal in G. Thus, if we can show that $P \cap Q = 1$, then we can use Theorem 9 from chapter 5 of Dummit and Foote to show that $PQ \cong P \times Q$. Say $x \in P \cap Q$. Then by Lagrange $|x||p$ and $|x||q$. Since $(p, q) = (19, 53) = 1$, we have that $|x| = 1$, so that $|P \cap Q| = 1$ and $P \cap Q = 1$. Thus, $PQ \cong P \times Q$. The only group of prime order is the cyclic group; thus, P and Q are cyclic, and $P = \langle x \rangle$, $Q = \langle y \rangle$ for some generators x, y.

We have $(x, y) \in P \times Q$. If $(x, y)^n = (1, 1)$, then $(x^n, y^n) = (1, 1)$, which implies that $p|n$ and $q|n$. Also, $|(x, y)||pq$, so $|(x, y)| = pq$ and $|P \times Q| = pq$. Since both $P \times Q$ and $\mathbb{Z}/(1007)$ are cyclic and $|P \times Q| = |\mathbb{Z}/(1007)|$, we have that $P \times Q \cong \mathbb{Z}/(1007)$ and we can conclude that $PQ \cong \mathbb{Z}/(1007)$, where P, Q are normal. It follows that PQ, and hence $\mathbb{Z}/(1007)$ are normal in G. Also, 1007 and 2 are coprime, so $\mathbb{Z}/(1007) \cap \mathbb{Z}/(2)$ is trivial.

Let $\phi : \mathbb{Z}/(2) \to \mathrm{Aut}(\mathbb{Z}/(1007)) \cong (\mathbb{Z}/(1007))^\times$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Also, HK is a subgroup of G. Since $|HK| = |G|$, we have $HK = G$, and it follows from Theorem 12 from chapter 5 in Dummit and Foote that,

$$G = HK \cong H \rtimes_\phi K.$$

In other words, any group G of order 2014 is isomorphic to a semidirect product $\mathbb{Z}/(1007) \rtimes_\phi \mathbb{Z}/(2)$.

(b) For any homomorphism $\phi : \mathbb{Z}/(2) \to \mathbb{Z}/(1007) \cong (\mathbb{Z}/(1007))^\times$ with $\phi(h) = xh$, x must be such that $x^2 \equiv 1 \mod 1007$, so there are four possible maps, particularly,

$$\phi_1 : h \mapsto h, \quad \phi_2 : h \mapsto 476h, \quad \phi_3 : h \mapsto 531h, \quad \text{and} \quad \phi_4 : h \mapsto 1006h.$$

Since ϕ_1 is the trivial map, using this homomorphism to define the semi-direct product $\mathbb{Z}/(1007) \rtimes_{\phi_1} \mathbb{Z}/(2)$ gives the direct product $\mathbb{Z}/(1007) \times \mathbb{Z}/(2)$, which is abelian. The other three maps are nontrivial, so the semi-direct products defined with them will be nonabelian. Thus, we need to show that $\mathbb{Z}/(1007) \rtimes_{\phi_2} \mathbb{Z}/(2)$, $\mathbb{Z}/(1007) \rtimes_{\phi_3} \mathbb{Z}/(2)$, and $\mathbb{Z}/(1007) \rtimes_{\phi_4} \mathbb{Z}/(2)$ are not isomorphic to one another. We'll call these groups G_2, G_3, and G_4 respectively in order to simplify the notation. In G_2, an element $(h, 1)$ has order 2 if $h + \phi_2(h) \equiv 1 \mod 1007$, or $h + 476h \equiv 477h \equiv 0 \mod 1007$, so $h = 19n$ with $n \in \mathbb{Z}$. Since $1007/19 = 53$, there are 53 elements of order 2 in G_2.

In G_3, we have $h + 531h \equiv 532h \equiv 0 \mod 1007$, so $h = 53n$ for $n \in \mathbb{Z}$ so there are $1007/52 = 19$ elements of order 2 in G_3. In G_4, we have $h + 1006h \equiv 1007h \equiv 0 \mod 1007$, so there is one element of order 2 in G_3. Since G_2, G_3, G_4 all have a different number of elements of order 2, they must non-isomorphic. Since G_1 is abelian and G_2 is nonabelian, they also cannot be isomorphic—G_1 cannot be isomorphoic to any of the others because the others are all nonabelian.

Exercise 3. Let R be a non-zero commutative ring. Set

$$\mathrm{Aff}(R) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in R^\times, b \in R \right\},$$

which is a group under matrix multiplication. Let I be the ideal in R generated by all $u - 1$ for $u \in R^\times$. That is, I is the set of finite sums $\sum_{i=1}^m r_i(u_i - 1)$ where $m \geq 1$, $r_i \in R$ and $u_i \in R^\times$. (For example, since $-1 \in R^\times$, I contains $-1 - 1 = -2$, so $2R \subset I \subset R$. Thus $I = R$ if $2 \in R^\times$, but if $2 \notin R^\times$ then I could be a proper ideal.)

(a) If the group $R^\times$ is finitely generated by $u_1, \ldots, u_n$, show $I = (u_1 - 1, \ldots, u_n - 1)$. This is *not* needed for later parts, but just gives an example of what I can look like for some rings.

(b) Show the commutator subgroup of $\mathrm{Aff}(R)$ is $\left(\begin{smallmatrix} 1 & I \\ 0 & 1 \end{smallmatrix}\right) = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in I\}$.

(c) Show the center of $\mathrm{Aff}(R)$ is $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : bI = (0)\}$.

Solution 3.

(a) Each $x \in I$ is a finite sum, and for each term x_i in x, we have $x_i = r_i(v_i - 1)$, where $r_i \in R$ and $v_i \in R^\times$. If $x_i \neq 0$, then $v_i \neq 1$, and since $u_1, ..., u_n$ generates $R^\times$, we have $v_i = u_1^{e_1} \cdot ... \cdot u_n^{e_n}$ where $e_1, ..., e_n \in \mathbb{Z}$, $e_j \neq 0$, and $u_j \neq 1$ for some $j \in 1, ..., n$. Now,

$$\begin{aligned} x_i = r_i(v_i - 1) &= r_i(u_1^{e^1} \cdot ... \cdot u_j^{e_j} \cdot ... \cdot u_n^{e_n} - 1) \\ &= r_i(u_j - 1)(u_1^{e^1} \cdot ... \cdot u_j^{e_j - 1} \cdot ... \cdot u_n^{e_n} - \frac{1}{u_j - 1} + \frac{u_1^{e^1} \cdot ... \cdot u_j^{e_j - 1} \cdot ... \cdot u_n^{e_n}}{u_j - 1}), \end{aligned}$$

as $u_j \neq 1$ and $u_j, 1 \in R^\times$. Set $\lambda_j = r_i(u_1^{e^1} \cdot ... \cdot u_j^{e_j-1} \cdot ... \cdot u_n^{e_n} - \frac{1}{u_j-1} + \frac{u_1^{e^1} \cdot ... \cdot u_j^{e_j-1} \cdot ... \cdot u_n^{e_n}}{u_j-1})$. Thus, $\lambda_j \in R$ and $x_i = \lambda_j(u_j - 1)$ for some $j \in 1, ..., n$. If for some term x_k in x, we have $x_k = \lambda_k(u_j - 1)$, then set $t_j = \lambda_j + \lambda_k$. Combining all like terms in this way, we obtain the form $x = t_1(u_1 - 1) + ... + t_n(u_n - 1)$, where each $t_i \in R$ and where some of the t_i's may be zero. Now if the original term x_i is zero, then simply set $x_i = 0(u_1 - 1)$. We have just shown that for any $x \in I$, $x \in (u_1 - 1, ..., u_n - 1)$ and hence $I \subset (u_1 - 1, ..., u_n - 1)$.
If $x \in (u_1 - 1, ..., u_n - 1)$, then $x = r_1(u_1 - 1) + ... + r_n(u_n - 1) = \sum_{i=1}^n r_i(u_i - 1)$ where $n \geq 1$ (since R is non-zero so one of the u_i's must be non-zero and if $x = 0$, then we may set $x = 0(u_i - 1)$ and thus have a sum at least one term long), $r_i \in R$ and $u_i \in R^\times$. By definition, this means that $x \in I$ and we have that $I = (u_1 - 1, \ldots, u_n - 1)$ as desired.

(b) Let the commutator subgroup of $G = \mathrm{Aff}(R)$ be denoted by G'. For $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \in G$, we have,

$$\begin{aligned} \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)^{-1} &= \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1/a & -b/a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1/c & -d/c \\ 0 & 1 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} ac & ad+b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1/(ac) & -d/(ac)-b/a \\ 0 & 1 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 1 & d(a-1)+(-b)(c-1) \\ 0 & 1 \end{smallmatrix}\right) \quad \text{(Let } x = d(a-1) + (-b)(c-1).\text{)} \\ &= \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \end{aligned}$$

where $d, -b \in R$ and $a, c \in R^\times$ and so $x \in I$ and all commutators of of G are in $\left(\begin{smallmatrix} 1 & I \\ 0 & 1 \end{smallmatrix}\right)$ (i.e. $G' \subset \left(\begin{smallmatrix} 1 & I \\ 0 & 1 \end{smallmatrix}\right)$). If a matrix is in $\left(\begin{smallmatrix} 1 & I \\ 0 & 1 \end{smallmatrix}\right)$, then it is of the form $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ where $b \in I$. By (a), we have that $b = r_1(u_1 - 1) + ... + r_n(u_n - 1)$ for some $r_1, ..., r_n \in R$. Notice,

$$[\left(\begin{smallmatrix} u_1 & -r_2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u_2 & r_1 \\ 0 & 1 \end{smallmatrix}\right)] = \left(\begin{smallmatrix} u_1 & -r_2 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} u_2 & r_1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} u_1 & -r_2 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} u_2 & r_1 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & r_1(u_1-1)+r_2(u_2-1) \\ 0 & 1 \end{smallmatrix}\right).$$

Also, $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & x+y \\ 0 & 1 \end{smallmatrix}\right)$. Thus, if n is even, we have,

$$\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = [\left(\begin{smallmatrix} u_1 & -r_2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u_2 & r_1 \\ 0 & 1 \end{smallmatrix}\right)] \cdot [\left(\begin{smallmatrix} u_3 & -r_4 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u_4 & r_3 \\ 0 & 1 \end{smallmatrix}\right)] \cdot \ldots \cdot [\left(\begin{smallmatrix} u_{n-1} & -r_n \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u_n & r_{n-1} \\ 0 & 1 \end{smallmatrix}\right)].$$

If n is odd, then,

$$\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = [\left(\begin{smallmatrix} u_1 & -r_2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u_2 & r_1 \\ 0 & 1 \end{smallmatrix}\right)] \cdot [\left(\begin{smallmatrix} u_3 & -r_4 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u_4 & r_3 \\ 0 & 1 \end{smallmatrix}\right)] \cdot \ldots \cdot [\left(\begin{smallmatrix} u_n & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & r_n \\ 0 & 1 \end{smallmatrix}\right)].$$

because $[\left(\begin{smallmatrix} u_n & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & r_n \\ 0 & 1 \end{smallmatrix}\right)] = \left(\begin{smallmatrix} 1 & r_n(u_n-1) \\ 0 & 1 \end{smallmatrix}\right)$. Thus, $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ is always a finite product of commutators, meaning $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in G'$ and so the commutator subgroup of $\mathrm{Aff}(R)$ is $\left(\begin{smallmatrix} 1 & I \\ 0 & 1 \end{smallmatrix}\right) = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in I\}$.

(c) Let the matrix $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ be in the center of G. Then, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} a & b+1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b+a \\ 0 & 1 \end{smallmatrix}\right)$. This means that $b + 1 = b + a$, so $a = 1$. If $\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \in G$, then we also have $\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 1 & 1 \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} c & cb+d \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} c & d+b \\ 0 & 1 \end{smallmatrix}\right)$. Thus, $cb + d = d + b$, so

$$b(c-1) = d - d = 0.$$

Since $c \in R^\times$ is arbitrary, it must be true that $bI = (0)$. Thus, the center of G is contained in $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : bI = (0)\}$.
If we take arbitrary $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : bI = (0)\}$ and $\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \in G$, then we have

$$\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} c & d+b \\ 0 & 1 \end{smallmatrix}\right),$$

and

$$\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} c & d+cb \\ 0 & 1 \end{smallmatrix}\right).$$

Since $bI = (0)$, we have

$$d + b - (d + cb) = d - d + b - cb = 0 + b(1-c) = b(1-c) = 0.$$

Thus, $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ for all $\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \in G$ and $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ is in the center of G as desired. We conclude that the center of $G = \mathrm{Aff}(R)$ is $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : bI = (0)\}$.

Exercise 4.

Solution 4.

Exercise 5. In class, we have seen that $\mathbb{Z}[i]$ is a euclidean domain with respect to the norm. Here we will deal with $\mathbb{Z}[\sqrt{3}]$.

(a) Prove $\mathbb{Z}[\sqrt{3}]$ is euclidean with respect to the absolute value of the norm using the same method you have seen already for $\mathbb{Z}[i]$. (Hint: $|x^2 - 3y^2| \leq \max(x^2, 3y^2)$ because x^2 and $3y^2$ are both ≥ 0.)

(b) Factor $2013+5210\sqrt{3}$ into a product of irreducibles in $\mathbb{Z}[\sqrt{3}]$. (Hint: When you want to solve $x^2-3y^2 = \pm p$ for a prime number $p \neq 3$, you need to choose the sign on the right so that $\pm p \equiv 1 \bmod 3$, since if $\pm p \equiv 2 \bmod 3$ then $x^2 \equiv 2 \bmod 3$, which is impossible. Having chosen the sign correctly, use a computer to calculate $3y^2 \pm p$ for $y = 1, 2, 3, \ldots$ until it is recognizably a perfect square.)

(c) Verify that $(5 + 2\sqrt{3})(8 - 3\sqrt{3})$ and $(7 + 2\sqrt{3})(4 - \sqrt{3})$ are both prime factorizations of $22 + \sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$ and then determine how the factors are matched with each other up to explicit unit multiple.

Solution 5.

(a) Let $\alpha = a + b\sqrt{3}$ and $\beta = c + d\sqrt{3}$ be two elements of $\mathbb{Z}[\sqrt{3}]$, with $\beta \neq 0$. Then in the field $\mathbb{Q}(\sqrt{3})$ we have $\alpha/\beta = r + s\sqrt{3}$ where $r = (ac + bd)/(c^2 + d^2)$ and $s = (bc - ad)/(c^2 + d^2)$ are rational numbers. Let p be an integer closest to r and let q be an integer closest to s, so that $|r - p|$ and $|s - q|$ are at most 1/2. Let $\theta = (r-p) + \sqrt{3}(s-q)$ and set $\phi = \beta\theta$. Then, $\phi = \alpha - (p + q\sqrt{3})\beta$, so that $\phi \in \mathbb{Z}[\sqrt{3}]$ is a Gaussian integer and $\alpha = (p + q\sqrt{3})\beta + \phi$. Since

$$|N(\theta)| = |(r-p)^2 - 3(s-q)^2| \leq \max((r-p)^2, 3(s-q)^2) \leq 3/4,$$

the multiplicativity of the norm N implies that $N(\phi) = N(\theta)N(\beta) \leq 3/4N(\beta)$. Thus, $\mathbb{Z}[\sqrt{3}]$ is euclidean.

(b)

(c)