Math 476
Exam 3

Instructions: You will have 55 minutes to complete this exam. The credit given on each problem will be proportional to the amount of correct work shown. Answers without supporting work will receive little credit.
Work your exam on separate sheets of paper. Be sure to number each problem and put your name on each page.

1. (12 points) Prove that conjugacy is an equivalence relation on a group.

   Reflexive: Let $a \in G$. Notice that $e \cdot a \cdot e^{-1} = (ea)e = ae = a$. Therefore, $a \in cl(a)$, hence conjugacy is reflexive.

   Symmetric: Suppose $b \in cl(a)$. Then, for some $x \in G$, $b = xax^{-1}$. From this, we have $x^{-1}bx = a$. Thus $a \in cl(b)$. Hence conjugacy is symmetric.

   Transitive: Suppose $b \in cl(a)$ and $c \in cl(b)$. Then for some $x, y \in G$, $b = xax^{-1}$ and $c = yby^{-1}$. Then $c = y(xax^{-1})y^{-1} = (xy)a(xy)^{-1}$ [recall that $(xy)^{-1} = y^{-1}x^{-1}$]. Hence $c \in cl(a)$. Therefore, conjugacy is transitive.

   We have shown that conjugacy is reflexive, symmetric, and transitive. Thus conjugacy is an equivalence relation. Thus conjugacy is an equivalence relation.

2. Let G be a group with $|G| = 126$.

   (a) (5 points) If G has more than one Sylow-3 subgroup, how many does it have?

   First, notice that $126 = 2 \cdot 3^2 \cdot 7$. Let n_3 represent the number of distinct Sylow-3 subgroups of G. Recall that by Theorem 24.5, we must have $n_3 \equiv 1(mod 3)$. Then $n_3 = 1, 4, 7, 10, 13, 16, \cdots$.

   We also know from Theorem 24.5 that n_3 must divide 14. Hence we must have $n_3 = 1$ or $n_3 = 7$. Thus, if there is more than one Sylow-3 subgroup, we must have 7 of them.

   (b) (8 points) Show that G has at least one proper normal subgroup.

   Let n_7 denote the number of Sylow-7 subgroups of G. Then, again using Theorem 24.5, $n_7 \equiv 1(mod)7$, so $n_7 = 1, 8, 15, 22 \cdots$.

   We also know from Theorem 24.5 that n_7 must divide 18. Hence we must have $n_7 = 1$. Finally, applying the corollary to Theorem 24.5, since there is a unique Sylow-7 subgroup, this subgroup is normal in G. Since its order is 7 while the order of G is 126, we have found a proper normal subgroup of G.

3. Let $R = \mathbb{Z}_{30}$.

   (a) (6 points) Find a zero divisor in R and demonstrate that it is a zero divisor.

   Note than every non-unit is R is a zero divisor. For example, since $(6)(5) = 30 \equiv 0(mod 30)$, then 6 is a zero divisor in R.

(b) (6 points) Find an idempotent a with $a \neq 0$ and $a \neq 1$ and demonstrate that it is an idempotent.

There are several possible examples here. One possibility is 6. Since $6^2 = 36 \equiv 6(mod 30)$, then 6 is an idempotent element in R.

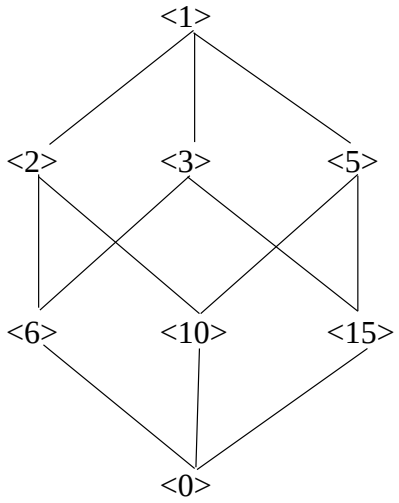
(c) (6 points) Find a unit a in R and demonstrate that it is a unit.

There are many examples here (any element that is relatively prime to 30 is a unit in this ring). One possibility is 11. Since $(11)(11) = 121 \equiv 1(mod 30)$, then 11 is a unit in R.

(d) (4 points) Find the characteristic of R.

Recall that, as proven in class, in a ring with unity, the characteristic of the ring is equal to the additive order of the unity in the ring. Here, the element 1 has order 30. Hence $charR = 30$.

(e) (8 points) Draw the ideal lattice for R. Use it to find the maximal ideals or R.



From the lattice diagram, we see that $\langle 2\rangle$, $\langle 3\rangle$, and $\langle 5\rangle$ are maximal ideals in R.

4. (12 points) Let $R = \mathbb{Z}_2[\sqrt{5}]$. Construct a multiplication table for the non-zero elements of this ring. Based on your table, is R an integral domain? Is it a field?

First, notice that $R = \mathbb{Z}_2[\sqrt{5}] = \{0, 1, \sqrt{5}, 1 + \sqrt{5}\}$. Then the multiplication table for the non-zero elements is:

	1	$\sqrt{5}$	$1+\sqrt{5}$
1	1	$\sqrt{5}$	$1+\sqrt{5}$
$\sqrt{5}$	$\sqrt{5}$	1	$1+\sqrt{5}$
$1+\sqrt{5}$	$1+\sqrt{5}$	$1+\sqrt{5}$	0

Notice that, since $(1 + \sqrt{5})(1 + \sqrt{5}) = 0$, then $1 + \sqrt{5}$ is a zero divisor. Hence R is not an integral domain. Also, since $1 + \sqrt{5}$ is a zero divisor, it is not a unit, hence R is also not a field (alternatively, every field is also an integral domain – see course notes or page 251 in your textbook).

5. (12 points) Let R be a ring and let A and B be ideals of R. Prove that $A \cap B$ is also an ideal of R.

   Let $x, y \in A \cap B$ and let $r \in R$. Consider $x - y$. Since A is an ideal, then $x - y \in A$. Similarly, since B is an ideal, $x - y \in B$. Therefore, $x - y \in A \cap B$ so $A \cap B$ is closed under addition.

   Next, consider rx. Since Since A is an ideal, then $rx \in A$. Similarly, since B is an ideal, $rx \in B$. Therefore, $rx \in A \cap B$.

   Finally, consider xr. Since Since A is an ideal, then $xr \in A$. Similarly, since B is an ideal, $xr \in B$. Therefore, $xr \in A \cap B$.

   Thus, by the ideal test, $A \cap B$ is an ideal of R.

6. (8 points) Let $R = \mathbb{Z}[x]$. Give an example of an infinite subset of R that is not an ideal of R. Justify your answer.

   There are many possible examples. All we need is an infinite subset of R that is not closed under either subtraction or under left or right ring multiplication. Here is one possibility:

   Let $S = \{p(x) : P(x) = ax^2 + bx + c \text{ for } a, b, c \in \mathbb{Z}\}$ (that is, the set of quadratic polynomials with integer coefficients).

   Notice that $p(x) = x^2 + 3x - 4$ is in S, and $x \in R$, but $xp(x) = x^3 + 3x^2 - 4x$ is not in S. This S is not an ideal of $\mathbb{Z}[x]$.

7. (10 points) Let $\phi : R \to S$ be a ring homomorphism. Prove **one** of the following properties of ring homomorphisms:

   (a) Let A be a subring of R. Then $\phi(A) = \{\phi(a) : a \in A\}$ is a subring of S.

   Let $s_1, s_2 \in \phi(A)$. Then $\exists r_1, r_1 \in A$ such that $\phi(r_1) = s_1$ and $\phi(r_2) = s_2$. Notice that since A is a subring of R, then $r_1 - r_2 \in A$ and $r_1 r_2 \in A$. With this in mind, $\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = s_1 - s_2 \in \phi(A)$. Similarly, $\phi(r_1 r_2) = \phi(r_1)\phi(r_2) = s_1 s_2 \in \phi(A)$.

   Since $\phi(A)$ is closed under both subtraction and multiplication, $\phi(A)$ is a subring of S.

   (b) $Ker\,\phi = \{r \in R : \phi(r) = 0\}$ is an ideal of R.

   First, since ϕ is a ring homorphism, it satisfies the group homomorphism property that $\phi(0) = 0$ [ϕ maps the additive identity to the additive identity]. Thus $Ker\,\phi \neq \emptyset$.

   Next, let $a, b \in Ker\,\phi$ and let $r \in R$. Then $\phi(a - b) = \phi(a) - \phi(b) = 0 - 0 = 0$. Thus $a - b \in Ker\,\phi$.

   Also, $\phi(ra) = \phi(r)\phi(a) = \phi(r)(0) = 0$. Similarly, $\phi(ar) = \phi(a)\phi(r) = \phi(0)(r) = 0$.

   Hence, by the ideal test, $Ker\,\phi$ is an ideal of R.

8. Let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$ be defined via $\phi(x) = 5x$.

(a) (6 points) Assuming that ϕ is a ring homomorphism, find $Ker\phi$.

Since $\mathbb{Z}_{12}$ us fairly small, we will check using direct computation.

$$\begin{array}{ll} \phi(0) = 5(0)(mod\,20) = 0(mod\,20) = 0. & \phi(6) = 5(6)(mod\,20) = 30(mod\,20) = 10 \\ \phi(1) = 5(1)(mod\,20) = 5(mod\,20) = 5. & \phi(7) = 5(7)(mod\,20) = 35(mod\,20) = 15 \\ \phi(2) = 5(2)(mod\,20) = 10(mod\,20) = 10. & \phi(8) = 5(8)(mod\,20) = 40(mod\,20) = 0 \\ \phi(3) = 5(3)(mod\,20) = 15(mod\,20) = 15. & \phi(9) = 5(9)(mod\,20) = 45(mod\,20) = 5 \\ \phi(4) = 5(4)(mod\,20) = 20(mod\,20) = 0 & \phi(10) = 5(10)(mod\,20) = 50(mod\,20) = 10 \\ \phi(5) = 5(5)(mod\,20) = 25(mod\,20) = 5 & \phi(11) = 5(11)(mod\,20) = 55(mod\,20) = 15 \end{array}$$

From these computations, we see that $Ker\,\phi = \{0, 4, 8\}$ [which is the ideal $\langle 4 \rangle$].

(b) (Extra Credit) Prove that ϕ is a ring homomorphism.

First note that to receive full credit on this problem, I expected you to carefully consider the effect of remainders modulo 12 and 20 on the computations. We were a little loose on this when we covered homomorphisms of groups, but we went back over these computations much more carefully in examples concerning homomorphisms of rings since the impact of modular arithmetic on multiplication is a bit more subtle.

Let $k, \ell \in \mathbb{Z}_{12}$. To simplify notation, suppose $k+\ell = 12m+r_1$ and $k\ell = 12n+r_2$ where $m, nin\mathbb{Z}$, $0 \leq r_1 < 12$ and $0 \leq r_2 < 12$.

Then $\phi(k + \ell) = \phi(12m + r_1) = \phi(r_1) = 5r_1 = 5(k + \ell - 12m) = 5k + 5\ell - 60m = 5k + 5\ell = \phi(k) + \phi(\ell)$.

Similarly, $\phi(k\ell) = \phi(12n + r_2) = \phi(r_2) = 5r_2 = 5(k\ell - 12n) = 5k\ell - 60n = 5k\ell = (5k)(5\ell) = \phi(k)\phi(\ell)$.

Note the all equalities above are $mod\,20$, and the second to last equality uses the fact that $5 \equiv 25(mod\,20)$.

Thus ϕ is a ring homomorphism.