Math 482, Abstract Algebra II, Spring 2012
Homework 10, due Tuesday 5/8

Read sections:
1. 5.2

Do the following problems:
1. 5.1: 19, 21, 41a (Note that I’m removing 41a from the assignment...you don’t need to write it up and turn it in).

2. Suppose that $R$ is a UFD, $B \subseteq R - \{0\}$ is a finite nonempty set. Prove that
   (i) if $b$ is an h.c.f. of $B$ and $b' \sim b$ then $b'$ is an h.c.f. of $B$.
   (ii) if $b, b'$ are h.c.f.s of $B$, then $b \sim b'$.

3. Suppose that $R$ is a UFD and $B \subseteq R = \{0\}$ is a finite nonempty set. Prove that an h.c.f. of $B$ exists.
   The following is a sketch of the proof. Since $R$ is a UFD, if $r \in R - \{0\}$ is not a unit, there are irreducibles $p_1, \ldots, p_n$ such that $r = p_1 \cdots p_n$ and the number of irreducibles appearing in any such expression is unique (this by definition). So we may define a function
   \[ \ell : R - \{0\} \to \mathbb{N} \]
   given by
   \[ \ell(r) = \begin{cases} n & \text{if } r \text{ is not a unit and can be decomposed into a product of } n \text{ irreducibles} \\ 0 & \text{if } r \text{ is a unit.} \end{cases} \]
   Conclude that $\ell(rs) = \ell(r) + \ell(s)$ for all $r, s \in R - \{0\}$. Conclude that $\ell(r) \leq \ell(s)$ if $r \mid s$ for all $r, s \in R - \{0\}$.

   Now let $T = \{ r \in R \mid r \text{ divides } b \text{ for all } b \in B \}$. We know $T \neq \emptyset$ since $1 \in T$.
   Conclude that $S = \{ \ell(r) \mid r \in T \}$ is bounded above. By the WOA (upside down—every bounded nonempty subset of $\mathbb{N}$ has a maximal element) we can find $a \in T$ be such that $\ell(a)$ is maximal in $S$.
   By construction $a \mid b$ for all $b \in B$. Suppose $c \mid b$ for all $b \in B$. We need to show that $c \mid a$.

   Repeating the construction above, let $T' = \{ r \in R \mid r \text{ divides } a \text{ and } c \}$ and $S' = \{ \ell(r) \mid r \in T' \}$. Again $T'$ is not empty and $S'$ is bounded, so there is a $d \in T$ such that $\ell(d)$ is as large as possible. Write $a = da_1$ and $c = dc_1$. If $c_1$ is a unit, conclude that $c \mid a$ as required. If $c_1$ is not a unit, then let $\pi$ be an irreducible divisor of $c_1$. Note that $\ell(d\pi) = \ell(d) + 1 > \ell(d)$, so that $d\pi$ does not divide both $a$ and $c$ (because $\ell(d)$ was as large as possible). Since $d\pi \mid c = dc_1$ it follows that $d\pi$ does not divide $a$. Conclude that $\pi$ does not divide $a_1$.

   Now for each $b \in B$, write $b = af_b = da_1f_b$ (we can do this since $a \mid b$ for all $b \in B$). Note that $\pi$ is prime since it is irreducible. We know that $c\pi \mid c$, and $c \mid b$, so $c\pi \mid b$ or $d_1\pi \mid da_1f_b$, that is $c_1\pi \mid a_1f_b$ or $\pi \mid a_1f_b$ for all $b \in B$. Since $\pi$ does not divide $a_1$ (as we saw above) it follows that $\pi \mid f_b$ for all $b \in B$. Conclude that $a\pi \mid b$ for all $b \in B$. This is a contradiction because $\ell(a\pi) = \ell(a) + 1 > \ell(a)$, but $\ell(a)$ was chosen to be maximal.

4. Suppose that $R$ is a UFD, $f, g \in \mathbb{R}[x] - \{0\}$. Prove that
(i) there is \( f_1 \in R[x] \) and \( \alpha \in R \) such that
- \( f = \alpha f_1 \)
- \( f_1 \) is primitive
- \( \alpha \) is an h.c.f. of \( f \).

(ii) if \( f = \alpha g \) for \( \alpha \in R \) and \( g \in R[x] \) primitive, then \( \alpha \) is an h.c.f. of \( f \). (A proof is given below, so you can skip this one).

(iii) if \( \alpha \) is an h.c.f. of \( f \) and \( \beta \) is an h.c.f. of \( g \), then \( \alpha \beta \) is an h.c.f. of \( fg \).

Here’s a proof of 4(ii), so you can see how they go.

Let \( \lambda \) be an h.c.f. of \( f \). It is enough so show (by problem 2(i) above) that \( \alpha \sim \lambda \). To that end, write \( f = a_n x^n + \cdots + a_0 \) and \( g = b_n x^n + \cdots + b_0 \). Of course \( f = \alpha g \) implies that \( a_i = \alpha b_i \), that is, \( \alpha \mid a_i = \alpha b_i \) for all \( i = 0, \ldots, n \). It follows (by definition) that \( \alpha \mid \lambda \), and thus that there there is some \( t \in R \) such that \( \lambda = \alpha t \). But since \( \lambda \mid a_i \), we have \( \alpha t \mid a_i \) for all \( i = 0, \ldots, n \). Let \( s \in R \) be such that \( \alpha ts = \alpha b_i \). Since \( R \) is an integral domain, we get that \( ts = b_i \), or \( t \mid b_i \) for all \( i = 0, \ldots, n \). But \( g \) is primitive, thus \( 1 \) is an h.c.f. of \( g \), and so \( t \mid 1 \) (by definition). We conclude that \( t \) is a unit so that \( \alpha \sim \lambda \) as required.

The grader will carefully consider 5.1.19, 4i.