Problem Set 4 (Due Friday, October 4)

Please see the course website for policy regarding collaboration and formatting your homework.

(30) In the ring $\mathbb{Z}[x]$, is 15 a unit, irreducible or a composite? What about in the ring $\mathbb{Q}[x]$?

(31) In the ring $\mathbb{Z}[\sqrt{-13}]$ show that 2, 7, $1+\sqrt{-13}$ and $1-\sqrt{-13}$ are irreducible. Which are prime?

(32) Let R be a UFD. For p a prime of R and f a nonzero element of R, let $v_p(f)$ be the exponent of p in the unique factorization of f. We formally set $v_p(0)=\infty$. Show that, for f and $g \in R$, we have $v_p(1)=0$, $v_p(f+g) \geq \min(v_p(f), v_p(g))$ and $v_p(fg)=v_p(f)+v_p(g)$ with the obvious treatment of ∞.

(33) Let k be a field and let $f(x)$ be an irreducible polynomial with coefficients in k. Show that $k[x]/f(x)k[x]$ is a field.

(34) Let A and B be commutative rings and $\phi : A \to B$ a ring homorphism:
 (a) Let $\mathfrak{p}$ be a prime ideal of B. Show that $\phi^{-1}(\mathfrak{p})$ is a prime ideal of A.
 (b) Give an example where $\mathfrak{m}$ is a maximal ideal of B but $\phi^{-1}(\mathfrak{m})$ is not a maximal ideal of A.

(35) Let R be a commutative ring and let $\mathfrak{p}$ be a prime ideal of R. Let $a(x)=\sum a_i x^i$ and $b(x)=\sum b_j x^j$ be polynomials with coefficients in R.
 (a) Suppose that $a(x)$ has at least one coefficient not in $\mathfrak{p}$, and that $b(x)$ has at least one coefficient not in $\mathfrak{p}$. Show that $a(x)b(x)$ has at least one coefficient not in $\mathfrak{p}$.
 (b) If you didn't solve Problem 25b last time, try again now. In other words, let $a(x)b(x)=\sum c_k x^k$, assume R is a UFD and show that $\mathrm{GCD}(c_k)=\mathrm{GCD}(a_i)\,\mathrm{GCD}(b_j)$.
 (c) Suppose that $a(x)$ is of the form $x^d+\sum_{i=0}^{d-1} a_i x^i$ and that $b(x)$ is of the form $x^e+\sum_{j=0}^{e-1} b_j x^j$. Let $a(x)b(x) = x^{d+e}+\cdots+\sum_{k=0}^{d+e-1} c_k x^k$. Suppose that d and $e>0$ and that $c_k \in \mathfrak{p}$ for $0 \leq k \leq d+e-1$. Show that $c_0 \in \mathfrak{p}^2$. (The contrapositive of this result is known as Eisenstein's Irreducibility Criterion.)

(36) Understanding how the Euclidean Algorithm works is pretty important, so do this exercise by hand (or at most, use a calculator/computer to check your arithmetic):
 (a) Let g be the GCD of 2019 and 594. Compute g using the Euclidean algorithm.
 (b) Find a product of elementary matrices $E_1, E_2, \ldots, E_r$ such $E_1 E_2 \cdots E_r \left[\begin{smallmatrix} 2019 \\ 594 \end{smallmatrix}\right] = \left[\begin{smallmatrix} g \\ 0 \end{smallmatrix}\right]$.
 (c) Find integers x and y such that $2019x+594y=g$.
 (d) ~~In the ring $\mathbb{Z}[i]$, use the Euclidean algorithm to find the GCD g_2 of $1+13i$ and 85. Find Gaussian integers x and y such that $(1+13i)x+85y=g_2$.~~ **Postponed until problem set 5.**
 (e) ~~In the ring $\mathbb{Q}[t]$, use the Euclidean algorithm to find the GCD g_3 of t^3+t and t^4-1. Find polynomials $x(t)$ and $y(t)$ such that $(t^3+t)x(t)+(t^4-1)y(t)=g_3$.~~ **Postponed until problem set 5.**

(37) Let k be a field and let $b_1(t), b_2(t), \ldots, b_r(t)$ be pairwise relatively prime polynomials in $k[t]$ and set $g(t) = b_1(t)b_2(t)\cdots b_r(t)$.
 (a) Show that the polynomials $g(t)/b_j(t)$ generate $k[t]/g(t)k[t]$ as a $k[t]$-module.
 (b) Let $f(t) \in k[t]$. Show that there are polynomials $a_1(t), a_2(t), \ldots, a_r(t)$, $c(t)$ in $k[t]$ such that

$$\frac{f(t)}{g(t)} = \sum_{j=1}^{r} \frac{a_j(t)}{b_j(t)} + c(t).$$

 Now you know why integration by partial fractions works!

(38) Let R be a PID. Note: Parts of this problem will probably appear in class, but we'll use these lemmas a lot, so please write out the proofs anyway.
 (a) Let x and $y \in R$ with $\mathrm{GCD}(x,y)=g$. Show that there is a matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with entries in R such that $ad-bc=1$ and $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = \left[\begin{smallmatrix} g \\ 0 \end{smallmatrix}\right]$.
 (b) Let $x_1, x_2, \ldots, x_n \in R$ with $\mathrm{GCD}(x_1, x_2, \ldots, x_n)=g$. Show that there is an $n \times n$ matrix A with entries in R such that $\det A = 1$ and $A\left[\begin{smallmatrix} x_1 & x_2 & \cdots & x_n \end{smallmatrix}\right]^T = \left[\begin{smallmatrix} g & 0 & \cdots & 0 \end{smallmatrix}\right]^T$. (Hint: Induct on n.)
 (c) Let x and y be nonzero elements of R. Show that there are invertible 2×2 matrices U and V with

$$U \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} V = \begin{bmatrix} \mathrm{GCD}(x,y) & 0 \\ 0 & \mathrm{LCM}(x,y) \end{bmatrix}.$$

 Here $\mathrm{LCM}(x,y) := \frac{xy}{\mathrm{GCD}(x,y)}$.