MATH 521A: Abstract Algebra
Homework 8 Solutions

1. * For nonzero polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, define the *content* of $f(x)$ as $c(f) = \gcd(a_n, a_{n-1}, \ldots, a_1, a_0)$. We call f *primitive* if $c(f) = 1$. Let $f(x), g(x) \in \mathbb{Z}[x]$. Suppose that $f(x), g(x)$ are both primitive. Prove that their product $f(x)g(x)$ is also primitive.

   Since f, g are primitive, $c(f) = c(g) = 1$. Suppose, by way of contradiction, that $c(fg) > 1$. Then some prime p divides each coefficient of fg. Now, p does not divide all the coefficients of f; suppose k is minimal so that $p \nmid a_k$ (and hence $p|a_0, p|a_1, \ldots, p|a_{k-1}$). Set $g(x) = b_n x^n + \cdots b_0$. Similarly, p does not divide all the coefficients of g; suppose j is minimal so that $p \nmid b_j$ (and hence $p|b_0, p|b_1, \ldots, p|a_{j-1}$). The coefficient of x^{k+j} in fg is $b_0 a_{k+j} + b_1 a_{k+j-1} + \cdots + b_{j-1} a_{k+1} + b_j a_k + b_{j+1} a_{k-1} + \cdots + b_{k+j} a_0$. All the terms to the left of $b_j a_k$ are multiples of p, because $b_0, \ldots, b_{j-1}$ are. All the terms to the right of $b_j a_k$ are multiples of p, because $a_0, \ldots, a_{k-1}$ are. But $b_j a_k$ is not a multiple of p, so the entire sum is not a multiple of p. But p divides every coefficient of fg, so we have a contradiction.

2. For nonzero $f(x), g(x) \in \mathbb{Z}[x]$, prove that $c(fg) = c(f)c(g)$.

   We have $f(x) = c(f)f'(x), g(x) = c(g)g'(x)$, where $f'(x)$ and $g'(x)$ have content 1. Now $f(x)g(x) = [c(f)c(g)]f'(x)g'(x)$. We take the content of the product, finding $c(fg) = c(f)c(g)c(f'g')$. By Problem 1 above, $c(f'g') = 1$, so $c(fg) = c(f)c(g)$.

3. * Let $f(x) \in \mathbb{Z}[x]$. Suppose that there are non-units $g(x), h(x) \in \mathbb{Q}[x]$ such that $f(x) = g(x)h(x)$. Then there are $g'(x), h'(x) \in \mathbb{Z}[x]$ such that $f(x) = g'(x)h'(x)$ and $\deg g(x) = \deg g'(x)$ (and also $\deg h(x) = \deg h'(x)$).

   Let a be the lcm of the denominators of the coefficients of g, and b the lcm of the denominators of the coefficients of h. Now, $abf(x), ag(x), bh(x) \in \mathbb{Z}[x]$ with $abf = (ag)(bh)$. By problem 2, $c(abf(x)) = c(ag(x))c(bh(x))$. But ab divides each coefficient of $abf(x)$, so $c(abf(x)) = c(f(x))ab$. Hence $ab|c(ag(x))c(bh(x))$. By the lemma below, we can write $ab = uv$ such that $u|c(ag(x))$ and $v|c(bh(x))$. Because $u|c(ag(x))$, u divides each coefficient of $ag(x)$, so we set $g'(x) = \frac{ag(x)}{u}, h'(x) = \frac{bh(x)}{v}$.

   Lemma: Let $a, b, c \in \mathbb{Z}$ with $a|bc$. There are $a', a'' \in \mathbb{Z}$ such that $a = a'a''$, $a'|b$, and $a''|c$. Proof: Use Fundamental Theorem of Arithmetic to write $a = p_1^{a_1} \cdots p_k^{a_k}, b = p_1^{b_1} \cdots p_k^{b_k}, c = p_1^{c_1} \cdots p_k^{b_k}$. Because $a|bc$, we have $a_i \le b_i + c_i$ for each $i \in [1, k]$. Now, set $d_i = \min\{b_i, a_i\}$ and $f_i = a_i - d_i$. Using these, we define $a' = p_1^{d_1} \cdots p_k^{d_k}$ and $a'' = p_1^{f_1} \cdots p_k^{f_k}$. We have $d_i + f_i = a_i$ so $a = a'a''$. By definition of d_i, $d_i \le b_i$, so $a'|b$. But also $f_i \le c_i$ so $a''|c$.

4. Fix $a \in \mathbb{Z}$ and consider $\phi_a : \mathbb{Z}[x] \to \mathbb{Z}[x]$ given by $\phi_a : f(x) \mapsto f(x-a)$. Prove that if $f(x)$ is reducible then $\phi_a(f(x))$ is reducible.

   If $f(x)$ is reducible then it is not the zero polynomial, and there are nonunit $g(x), h(x) \in \mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$. We have $\phi_a(f(x)) = \phi_a(g(x)h(x)) = \phi_a(g(x))\phi_a(h(x)) = g(x-a)h(x-a)$. Now, if $g(x)$ is a constant, then $g(x-a) = g(x)$, so $g(x-a)$ is still not a unit. If instead $g(x)$ is a non-constant polynomial, then $g(x-a)$ is also a non-constant polynomial of the same degree, so again is not a unit. Similarly, $h(x-a)$ is not a unit, so $\phi_a(f(x))$ is reducible.

5. Use Eisenstein's criterion (and Problem 4, if necessary) to prove that x^5+5x+2 is irreducible in $\mathbb{Q}[x]$.

   Set $f(x) = x^5+5x+2$, and consider instead $f(x+3) = x^5+15x^4+90x^3+270x^2+410x+260$. Note that 5 divides each of $15, 90, 270, 410, 260$, but $5 \nmid 1$ and $5^2 \nmid 260$. Hence, by Eisenstein's criterion, $f(x+3)$ is irreducible. By Problem 4, since $f(x+3) = \phi_3(f(x))$, also $f(x)$ must be irreducible.

   You could also consider $f(x-2) = x^5-10x^4+40x^3-80x^2+85x-40$, also with 5.

6. Fix p prime, and consider the "natural map" $\phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ given by $\phi_p : a_nx^n + \cdots + a_1x + a_0 \mapsto [a_n]_px^n + \cdots + [a_1]_px + [a_0]_p$. Prove that if $p \nmid a_n$ and $f(x)$ is primitive and reducible, then $\phi_p(f(x))$ is also reducible.

   Since f is reducible, there are $g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$. Since f is primitive, neither g nor h are constants. Neither of the leading coefficients of g, h are multiples of p, since the leading coefficient of f isn't. Hence $\deg(\phi_p(g)) = \deg(g) > 0$ and similarly $\deg(\phi_p(h)) = \deg(h) > 0$. Hence $\phi_p(f) = \phi_p(g)\phi_p(h)$, a product of nonunits.

7. Use Problem 6 to prove that $f(x) = x^3+5x+4$ is irreducible in $\mathbb{Z}[x]$.

   Taking $p = 3$, we get $\phi_3(f) = x^3+2x+1$. Plugging in $0, 1, 2$, we get 1 each time (in $\mathbb{Z}_3$). Hence $\phi_3(f)$ is irreducible in $\mathbb{Z}_p[x]$. Since $f(x)$ is primitive and 3 does not divide the leading coefficient, $f(x)$ is irreducible in $\mathbb{Z}[x]$.

8. Set $f(x) = 3x^3+4x^2+7x+2$. Show that this is reducible in $\mathbb{Z}[x]$ but irreducible in $\mathbb{Z}_3[x]$. Does this contradict problem 6?

   We have $f(x) = (3x+1)(x^2+x+2)$ in $\mathbb{Z}[x]$, so f is reducible over $\mathbb{Z}$. However $(3x+1)$ is a unit in $\mathbb{Z}_3[x]$, so this does not prove $\phi_3(f)$ is reducible. In fact, $f(0) = 2, f(1) = 1, f(2) = 2$. Hence $f(x)$ has no linear factor in $\mathbb{Z}_3[x]$. Since $\deg(f) = 2$ in $\mathbb{Z}_3[x]$, it is irreducible. Problem 6 doesn't apply since $p = 3$ divides the leading coefficient of f.

9. Factor x^4-25 in $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$.

   Over $\mathbb{Q}$, this factors as $(x^2-5)(x^2+5)$, two irreducibles (verified by Eisenstein's criterion with $p = 5$). Over $\mathbb{R}$, this factors as $(x-\sqrt{5})(x+\sqrt{5})(x^2+5)$, three irreducibles (verified by discriminant $b^2-4ac = -20 < 0$). Over $\mathbb{C}$, this factors as $(x-\sqrt{5})(x+\sqrt{5})(x-\sqrt{5}i)(x+\sqrt{5}i)$, four irreducibles.

10. Factor $x^3-ix^2+5x-5i$ in $\mathbb{C}[x]$.

    Trial and error, and long division in $\mathbb{C}[x]$ is what's needed here. Luckily i is a root, so we can divide by $(x-i)$ to get x^2+5. Hence the polynomial factors as $(x-i)(x-\sqrt{5}i)(x+\sqrt{5}i)$.