WORKSHEET # 8

MATH 435 SPRING 2011

For this worksheet, we assume all rings are commutative, associative and with multiplicative identity. We assume that all homomorphisms send 1 to 1.

1. Suppose that k is a field and $f(x) \in k[x]$. Fix an element $a \in k$. Prove that $f(a) = 0$ if and only if $(x - a)|f(x)$. Conclude that if $f(x) \in k[x]$ is reducible (not irreducible) and has degree ≤ 3, then $f(x)$ has a root in k.
Hint: The $\Leftarrow$ direction should be really easy. For the other direction, consider the remainder of $f(x)/(x - a)$.

Solution: Suppose first that $(x-a)|f(x)$. Thus $f(x) = g(x)(x-a)$. Thus $f(a) = g(a)(a-a) = g(a) \cdot (0) = 0$ and the $\Leftarrow$ direction is proven.

Conversely, suppose that $f(a) = 0$. Now, $f(x) = (x - a)q(x) + r(x)$ where $r(x)$ is the remainder obtained by dividing $f(x)$ by $(x-a)$. Thus the degree of $r(x)$ is < 1. It follows that $r(x)$ is a constant function, ie $r(x) \in k$. Now, plug in $x = a$ to get $0 = f(a) = (a - a)q(a) + r(a) = 0 + r(a) = r(a)$. Thus $r(a) = 0$, and so $r(x) = 0$ (since $r(x)$ is a constant).

For the conclusion, suppose that $f(x)$ is reducible, and $f(x) = g(x)h(x)$ with $\deg g, h > 0$. Since $\deg f(x) \leq 3$, this implies that either g or h has degree 1, so one of them is of the form $(ax - b)$ for some $a, b \in k$ with $a \neq 0$. But then $(x - \frac{a}{b})$ also divides $f(x)$ and so f has a root $\frac{a}{b}$ in k.

Definition 0.1. The *content* of a non-zero polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is the gcd of the a_i's. A polynomial in $\mathbb{Z}[x]$ is called *primitive* if it has content equal to 1.

2. [Gauss's Lemma] Prove that product of primitive polynomials is primitive.
Hint: Suppose p is a prime divisor of the coefficients of $f(x)g(x)$. Consider $f_p(x)$ and $g_p(x)$, by viewing the polynomials mod p in $\mathbb{Z}_{\text{mod}p}[x]$. Compare then $f_p(x)$, $g_p(x)$ and $(f(x)g(x))_p = f_p(x)g_p(x)$.

Solution: Suppose that $f(x)g(x)$ is not primitive and that p is a prime that divides the content of p. Notice that the map $\pi : \mathbb{Z}[x] \to \mathbb{Z}_{\text{mod}p}[x]$ is a ring homomorphism. Now, $\pi(f(x)g(x)) = (f(x)g(x))_p = \pi(f(x))\pi(g(x)) = f_p(x)g_p(x)$. Since p divides the content of $(f(x)g(x))$, we know that $(f(x)g(x))_p = 0$. Thus $f_p(x)g_p(x) = 0$. But $\mathbb{Z}_{\text{mod}p}[x]$ is an integral domain, so that means either $f_p(x) = 0$ or $g_p(x) = 0$. In the first case, p divides the content $f(x)$, in which case $f(x)$ is not primitive. In the second case, p divides the content of $g(x)$. Thus in either case, we have a contradiction and are done.

3. Suppose that $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible as an element of $\mathbb{Q}[x]$, then show it is also reducible in $\mathbb{Z}[x]$. *Hint:* Reduce to the case where f is primitive and then suppose $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Q}[x]$. Then clear the denominators of g and h and pay attention to the "content".

Solution: First suppose that f is not primitive. Then $f(x) = \lambda \overline{f}(x)$ for some non-zero non-unit $\lambda \in \mathbb{Z}$ (the content of f). Thus f is reducible (not that λ is not a unit in $\mathbb{Z}$ even though it is a unit in $\mathbb{Q}$). Thus we only have to consider the case of f primitve.

Using the notation from the hint, choose $a, b \in \mathbb{Q}$ such that $ag(x)$ and $bh(x)$ are primitive polynomials in $\mathbb{Z}[x]$ (for example, choose $a = c/d$ where c is the lcm of the denominators of the coefficients of g and d is the gcd of the numerators of the coefficients of d). Now,

$$f(x) = \frac{1}{ab}(ag(x))(bh(x)).$$

The product $(ag(x))(bh(x)) = m(x) \in \mathbb{Z}[x]$ is a primitive polynomial by the previous exercise. Thus we have $f(x) = \lambda m(x)$ for some $\lambda \in \mathbb{Q}$ where both f and m are primitive. The only way this can happen is if λ is a unit in $\mathbb{Z}$ (ie, $\lambda = \pm 1$). Thus $f(x) = (ag(x))(bh(x))$ is also a factorization in $\mathbb{Z}[x]$ and so $f(x)$ is not irreducible.

4. Suppose $f(x) \in \mathbb{Z}[x]$ is an polynomial of degree ≥ 1 and $p \in \mathbb{Z}$ is a prime number. Suppose that $\deg f_p(x) = \deg f(x)$ (where $f_p(x)$ is the polynomial obtained by reducing the coefficients modulo p as above). Show that if $f_p(x)$ is irreducible, then $f(x)$ is also irreducible.

Solution: We prove the contrapositive. Suppose that $f(x)$ is reducible and write $f(x) = g(x)h(x)$ with $\deg g, h > 0$. Since $\deg f_p(x) = \deg f(x)$, the leading coefficient of f is not divisible by p. Thus the leading coefficients of g and h (whose product is the leading coefficient of f) is also not divisible by p. Thus $\deg g(x) = \deg g_p(x)$ and $\deg h(x) = \deg h_p(x)$ as well. Now, using the notation from the solution to problem **2.**,

$$f_p(x) = \pi(f(x)) = \pi(g(x)h(x)) = \pi(g(x))\pi(h(x)) = g_p(x)h_p(x).$$

Because $g_p(x)$ and $h_p(x)$ have the same degree as g and h, they cannot be units, and so $f_p(x)$ is also reducible.

5. Apply problem # **4.** to $f(x) = 21x^3 - 3x^2 + 2x + 9$ to prove that $f(x)$ is irreducible as an element of $\mathbb{Q}[x]$. Do the same for the polynomial $g(x) = x^5 + 2x + 4$.

Solution: For $f(x)$, I set $p = 2$ and consider $f_p(x) = (21x^3 - 3x^2 + 2x + 9) \mod 2 = x^3 + x^2 + 1$. If $f_p(x)$ was reducible, then it would have a root in $\mathbb{Z}_{\text{mod } 2}$ because its degree is ≤ 3. Thus either $f_p(0) = 0$ or $f_p(1) = 0$. But those are not zero (plug it in, in both cases you get $1 \neq 0$). Thus by **4.**, $f(x) \in \mathbb{Z}[x]$ is irreducible so by **3.**, $f(x) \in \mathbb{Q}[x]$ is also irreducible.

Now we consider $g(x)$. I we set $p = 3$ and work modulo 3. In that case $g_p(x) = x^5 + 2x + 1$. First we check whether $g_p(x)$ has a root. $g_p(0) = 1 \neq 0$, $g_p(1) = 1 + 2 + 1 \equiv_3 1 \neq 0$ and $g_p(2) = 32 + 4 + 1 \equiv_3 1$. This also shows that $g_p(x)$ has no linear factors. Thus if it can be factored, we can write

$$\begin{aligned} x^5 + 2x + 1 &= (ax^2 + bx + c)(dx^3 + ex^2 + fx + i) \\ &= adx^5 + (ae + db)x^4 + (af + eb + cd)x^3 + (ai + bf + ce)x^2 + (bi + fc)x + ci, \end{aligned}$$

with $a, d \neq 0$. Without loss of generality, we may assume that $a = 1$, which implies that $d = 1$ as well (since $adx^5 = x^5$). Thus

$$x^5 + 2x + 1 = x^5 + (e + b)x^4 + (f + eb + c)x^3 + (i + bf + ce)x^2 + (bi + fc)x + ci.$$

Therefore $e = -b$. Furthermore, since $ci = 1$, we must have $i = c = 1$ or $i = c = 2$, so in either case, $c = i$. Plugging this in, we get:

$$x^5 + 2x + 1 = x^5 + (f - b^2 + c)x^3 + (c + bf - cb)x^2 + (bc + fc)x + 1$$

Therefore, $f - b^2 + c = 0$ and $c + bf - cb = 0$ and $bc + fc = 2$. Plugging in $f = b^2 - c$ into the other two equations yields:

$$0 = c + b^3 - bc - cb = c + b^3 + cb, \text{ and } bc + cb^2 - c^2 = 2.$$

Now we have two equations and two unknowns, b, c. At this point we can just apply brute-force. We first try $c = 1$ (remember, $c = 1$ or 2). So plugging this into the second equation gives $b + b^2 - 1 = 2$. The only solutions to that are $b = 0, 2$. However $b = 0, c = 1$ is not a solution to the first equation $0 = c + b^3 + cb$. Likewise $b = 2, c = 1$ is not a solution to $0 = c + b^3 + cb$ since $1 + 8 + 2 \equiv_3 2 \neq 0$.

Now we try $c = 2$. Plugging this into the first equation gives $0 = 2 + b^3 + 2b$. Certainly $b = 0$ is not a solution, $b = 1$ is also not a solution and if we set $b = 2$, then $2 + 8 + 4 = 14 \equiv_3 2 \neq 0$. Thus $c = 2$ is also impossible. This proves that f_p is irreducible and thus $f(x)$ is also irreducible in $\mathbb{Z}[x]$ and thus also in $\mathbb{Q}[x]$.