MODERN ALGEBRA II SPRING 2013: TENTH PROBLEM SET

1. We have seen that the ring $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, and that the units $(\mathbb{Z}[\sqrt{-3}])^* = \{\pm 1\}$. Show that the polynomial x^2+x+1 is irreducible in $\mathbb{Z}[\sqrt{-3}][x]$ but not in $\mathbb{Q}(\sqrt{-3})[x]$. (First show that x^2+x+1 has a root in $\mathbb{Q}(\sqrt{-3})$ but not in $\mathbb{Z}[\sqrt{-3}]$. Then show that, if there is a factorization $x^2+x+1 = (ax+b)(cx+d)$ with $a, b, c, d \in \mathbb{Z}[\sqrt{-3}]$, then a and c are units, contradicting the fact that there is no root of x^2+x+1 in $\mathbb{Z}[\sqrt{-3}]$. Finally, rule out a factorization of the form $x^2+x+1 = rg(x)$ where $r \in \mathbb{Z}[\sqrt{-3}]$ is not a unit. For a slightly more involved, but also more germane example, one can show that $3x^2+4x+3$ is irreducible in $\mathbb{Z}[\sqrt{-5}][x]$ but not in $\mathbb{Q}(\sqrt{-5})[x]$.)

2. Test the following polynomials in $\mathbb{Z}[x]$ for irreducibility in $\mathbb{Q}[x]$ and in $\mathbb{Z}[x]$. In each case, give a reason why the polynomial is irreducible or find its complete factorization in $\mathbb{Q}[x]$ and in $\mathbb{Z}[x]$.

   (a) $2x^4 - 50x^3 + 100x^2 - 750x + 60$; (b) $x^3 - 2x^2 + x + 1$
   (c) $2x^3 + 3x^2 + 3x + 1$; (d) $x^4 + 5x^2 + 6$; (e) $3x^{27} - 84$.

3. Let F be a field and let $a, b \in F$ with $a \neq 0$. Show that $f(x) \in F[x]$ is irreducible if and only if $f(ax+b)$ is irreducible.

4. (i) Let F be a field, and let $f(x) = x^4 + c$, where $c \in F$. Show that $x^2 + ax + b$ is a factor of $f(x)$ if and only if $x^2 - ax + b$ is a factor of $f(x)$. Further show that, if $x^2 + b$ is a factor of $f(x)$, then so is $x^2 - b$. Conclude that $f(x)$ is not irreducible if and only if either $-c$ is a square in F or $c = b^2$ is the square of an element $b \in F$ such that $2b$ is also the square of an element of F. In particular, show that $x^4 + 4$ is reducible in $\mathbb{Q}[x]$ and find an explicit factorization of it.

   (ii) More generally, suppose that $f(x) = x^4 + c_1x^2 + c_2 \in F[x]$. As in Part (i), show that x^2+ax+b is a factor of $f(x)$ if and only if x^2-ax+b is a factor of $f(x)$ and show that, if $f(x) = (x^2+ax+b)(x^2-ax+b)$, then $c_2 = b^2$ and $c_1 = 2b - a^2$. Conclude that $f(x) = (x^2+ax+b)(x^2-ax+b)$ if and only if c_2 is a square, and there exists a square root b of c_2 such that $2b - c_1$ is a square.

   (iii) Again with $f(x) = x^4 + c_1x^2 + c_2 \in F[x]$, show that $f(x) = (x^2+a)(x^2+b)$ if and only if $c_1^2 - 4c_2$ is a square in F.

5. Let $f(x) \in \mathbb{Z}[x]$ be the polynomial $x^4 - 10x^2 + 1$. For a prime number p, we let $\bar{f}(x)$ be the reduction mod p of $f(x)$. The goal of this problem is to show that $\bar{f}(x)$ is reducible for all p, but that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

   (i) Working mod p, and using Part (ii) of the previous problem, show that, if either 2 or 3 is a square in $\mathbb{Z}/p\mathbb{Z}$, then $\bar{f}(x)$ has a factorization
   $$\bar{f}(x) = (x^2 + ax + b)(x^2 - ax + b).$$

   (ii) Using Part (iii) of the previous problem, show that $\bar{f}(x)$ has a factorization
   $$\bar{f}(x) = (x^2 + c)(x^2 + d)$$
   if and only if 6 is a square in $\mathbb{Z}/p\mathbb{Z}$.

   (iii) Show that, in $\mathbb{Z}/p\mathbb{Z}$, if neither 2 nor 3 is a square, then their product $6 = 2 \cdot 3$ is a square. (Hint: This follows from the fact that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, and is a consequence of the following fact about cyclic groups, written additively: Let n be **even** and let $G = (\mathbb{Z}/n\mathbb{Z}, +)$ be the usual additive cyclic group of order n. let $H = 2(\mathbb{Z}/n\mathbb{Z}) = \langle 2 \rangle$ be the subgroup of all elements which are twice an element. Then $(G : H) = 2$, and hence the sum of two elements not in H lies in H. Thus, if two elements in $(\mathbb{Z}/p\mathbb{Z})^*$ are not squares, then their product is always a square.) Hence there is a factorization of $\bar{f}(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ for every prime p.

   (iv) Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$. (Hint: First, $f(x)$ has no root (why?), so it can only factor as a product of two quadratic polynomials. Using the previous problem, if $x^2 + ax + b$ is an irreducible factor of $f(x)$, then so is $x^2 - ax + b$, and so if $a \neq 0$ then $f(x) = (x^2 + ax + b)(x^2 - ax + b)$ by counting degrees. Otherwise $f(x) = (x^2 + c)(x^2 + d)$ for some $c, d \in \mathbb{Q}$. Now use the previous problem again and the fact that $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ are all irrational.)

   Note: One can analyze more generally those polynomials $f(x) \in \mathbb{Z}[x]$ such that the mod p reduction $\bar{f}(x)$ is reducible for every prime p, but $f(x)$ is irreducible in $\mathbb{Q}[x]$. In spite of the above example, factoring integer polynomials, which is an important theoretical and practical question, can be done effectively, and reduction mod p for large primes p is an important step in many algorithms.