Modern Algebra II: Problem Set 10

Nilay Kumar

Last updated: April 15, 2013

Problem 1

Take the polynomial $f(x) = x^2 + x + 1$. Let us find a root of this polynomial in $\mathbb{Q}(\sqrt{-3})[x]$:

$$\begin{aligned} 0 &= (p + q\sqrt{-3})^2 + p + q\sqrt{-3} + 1 \\ &= p^2 - 3q^2 + p + 1 + (2p+1)b\sqrt{-3}, \end{aligned}$$

and thus there are two roots $-\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$. These coefficients are clearly not integers and thus we have solutions that are not in $\mathbb{Z}(\sqrt{-3})$. Consequently, $f(x)$ is not irreducible in $\mathbb{Q}(\sqrt{-3})[x]$. Now suppose that we can factor $x^2 + x + 1 = (ax+b)(cx+d)$ with $a, b, c, d \in \mathbb{Z}[\sqrt{-3}]$. Expanding, we find that $ac = 1$, i.e. a, c must be units. The units are ± 1, and thus b, d (up to a minus sign) are roots of f, and we reach a contradiction. Finally, we cannot factor $f(x) = rg(x)$ where $r \in \mathbb{Z}[\sqrt{-3}]$ is not a unit, as we would have to have $a_i r = 1$ for $i = 0, 1, 2$, i.e. r would be a unit. Consequently, we cannot factor anything out of $x^2 + x + 1$ in $\mathbb{Z}[\sqrt{-3}][x]$, and thus f is irreducible in this ring.

Problem 2

(a) Let $f(x) = 2x^4 - 50x^3 + 100x^2 - 750x + 60$. Note that f is Eisenstein at 5, as (5) is a prime ideal, 2 does not divide 5 and 25 does not divide 60. Thus f is irreducible as an element of $\mathbb{Q}[x]$. Note, additionally, that we can factor out a 2 from $f(x)$, and thus f is not irreducible in $\mathbb{Z}[x]$, and thus factors as $f(x) = 2(x^4 - 25x^3 + 50x^2 - 375x + 30)$.

(b) Let $f(x) = x^3 - 2x^2 + x + 1$. If we examine f in $\mathbb{F}_2[x]$, we find that $\bar{f}(x) = x^3 + x + 1$, which is irreducible as it has no root in $\mathbb{F}_2$. By the theorem proved in class, then $f(x)$ is irreducible in $\mathbb{Q}[x]$. By exactly the same reasoning as the first problem, we see that in $\mathbb{Z}[x]$ the polynomial does not factor as $(ax+b)(cx+d)$ or as $rg(x)$. Consequently, f is also irreducible in $\mathbb{Z}[x]$.

(c) Let $f(x) = 2x^3 + 3x^2 + 3x + 1$. By the rational roots test, we are motivated to test $-1/2$ as a root, as a positive number will clearly not yield zero, and because the numerator must divide the constant term and the denominator must divide the leading coefficient. It turns out that $x = -1/2$ is indeed a root of f, and thus $f(x)$ is reducible in $\mathbb{Q}[x]$. Furthermore, we can long divide and show that $f(x)/(2x+1) = x^2+x+1$ and thus $f(x) = (2x+1)(x^2+x+1)$ and thus is not irreducible in $\mathbb{Z}[x]$.

(d) Let $f(x) = x^4+5x^2+6 = (x^2+2)(x^2+3)$. Clearly, then, f is reducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. This is, in fact, the complete factorization in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ because neither x^2+2 or x^2+3 has a root in $\mathbb{Q}$.

(e) Let $f(x) = 3x^{27} - 84$. f is not irreducible in $\mathbb{Z}[x]$ because we can factor out a 3. However, f is irreducible in $\mathbb{Q}[x]$, as it is Eisenstein at 4.

Problem 3

We prove the contrapositive. Suppose $f(x) = g(x)h(x)$ is reducible with the degrees of g, h greater than 0. Clearly, then $f(ax+b) = g(ax+b)h(ax+b)$ is reducible. The degrees of $g(ax+b)$ and $h(ax+b)$ are equal to the degrees of $g(x)$ and $h(x)$, just by term-by-term inspection (and because $a^n \neq 0$).

Conversely, suppose $f(ax+b) = g(x)h(x)$ is reducible. Now we simply change variables:

$$f(x) = g(a^{-1}x - a^{-1}b)h(a^{-1}x - a^{-1}b)$$

and find that $f(x)$ is reducible, again because the polynomials on the right hand side will have the same degree as they did before.

Problem 4

(i) Let $f(x) = x^4+c$. Suppose $g(x) = x^2+ax+b$ is a factor of $f(x)$. Then, as in the above problem, we can claim that $g(-x)$ factors $f(-x)$. But note that $f(-x) = f(x)$, and thus $g(-x) = x^2 - ax + b$ must factor $f(x)$. Note that then $f(x) = x^4+(b-a^2)x^2+b^2$ and thus $2b = a^2$. The converse argument follows almost identically. Now suppose that x^2+b is a factor of $f(x)$. Then we can write $f(x) = (x^2+b)(x^2+ex+f) = x^4+ex^3+(b+f)x^2+bex+bf$. Clearly we must have $e = 0$, $b+f = 0$, and $bf = c$, i.e. $-b^2 = c$. Consequently, $x^2 - b$ must also factor $f(x)$.

Thus if $c = b^2$ and $2b = a^2$, $f(x)$ cannot be irreducible as it is divisible by $x^2 \pm ax + b$. Similarly, if $c = -b^2$, $f(x)$ is not irreducible as it is divisible by $x^2 \pm b$. Conversely, note that if $f(x)$ is reducible into two quadratic polynomials. Then, if the linear term in one of these polynomials is zero, we must have by above, that $c = b^2$ for some $b \in F$, but if the linear term does not vanish, then $c = -b^2$ for some $b \in F$ and $2b = a^2$ for some $a \in F$.

(ii) Now suppose that $f(x) = x^4 + c_1x^2 + c_2$. Just as before, since $f(x) = f(-x)$, and if $g(x) = x^2 + ax + b$ factors $f(x)$ then $g(-x) = x^2 - ax + b$ must factor it as well. The algebra from before carries over identically and thus if f factors in this way, $c_2 = b^2$ and $c_1 = 2b - a^2$. Thus if c_2 is a square and there exists a square root b of c_2 such that $2b - c_1 = a^2$ is a square, $f(x)$ factors non-trivially as above. This shows that $f(x) = (x^2 + ax + b)(x^2 - ax + b)$ if and only if these conditions hold.

(iii) Let $f(x) = x^4 + c_1x^2 + c_2$ as above. By the quadratic formula on x^2 we can find two terms linear in x^2, $x^2 - a$ and $x^2 - b$, as long as the discriminant in the formula is a square in F.

Problem 5

(i) Let $f(x) \in \mathbb{Z}[x]$ be the polynomial $x^4 - 10x^2 + 1$. Using the notation from the previous problem, we have $c_1 = -10$ and $c_2 = 1$. Note that c_2 is a square of ± 1 and $2b - c_1 = 2(\pm 1) + 10$ is either 12 or 8. Since $12 = 2^2 \cdot 3$ and $8 = 2^3$, if either 2 or 3 are squares in $\mathbb{Z}/p\mathbb{Z}$, 12 and 8 can be written as squares, i.e. the previous result holds in this case: $\bar{f}(x) = (x^2 + ax + b)(x^2 - ax + b)$.

(ii) Using the third part of the previous problem we see that if $c_1^2 - 4c_2$ is a square, we can factor as desired. In our case we have $100 - 4 = 96 = 2^5 \cdot 3 = 2^4 \cdot 6$, and thus we can write $\bar{f}(x) = (x^2 + c)(x^2 + d)$ if and only if 6 is a square in $\mathbb{Z}/p\mathbb{Z}$.

(iii) By the given group theory hint we know that if two elements in $(\mathbb{Z}/p\mathbb{Z})^*$ are not squares, then their product is always a square. In our case, if 2 and 3 are not squares, then $2 \cdot 3 = 6$ must be a square and thus $\bar{f}(x) = (x^2 + c)(x^2 + d)$. On the other hand, if either 2 or 3 is a square, then $\bar{f}(x) = (x^2 + ax + b)(x^2 - ax + b)$ using the reasoning above.

(iv) By the rational root test, rational roots of $f(x)$ must be ± 1. However, neither of these actually is. Thus, $f(x)$ must factor as the product of two quadratics. But by the previous part, since 12 and 8 are note squares, and 96 is not a square, $f(x)$ cannot factor as the product of quadratics, either. Hence, $f(x)$ must be irreducible in $\mathbb{Q}[x]$.