Math 547/702I – Some Solutions

Frank Thorne

April 28, 2015

19.2. (g). Is $x^4 - 3x^2 + 6x + 1$ irreducible?

No, Eisenstein's criterion doesn't apply, even after the trick. This question requires a small amount of brute force.

It it were reducible, it would factor over $\mathbb{Z}$ by Gauss's lemma. First of all, check that it doesn't have any roots (and therefore no linear factors). For example, check directly that $x = -2, -1, 0, 1, 2$ are not roots, and then use an inequality to argue that if $|x| \geq 3$ the same is true.

Therefore, if it factored we would have

$$x^4 - 3x^2 + 6x + 1 = (x^2 + ax + b)(x^2 + cx + d).$$

But $a = -c$ (why?) and $bd = 1$, so $b = d = 1$ or $b = d = -1$. Keep going along these lines to obtain a contradiction.

20.6 (a). This is basically (part of) Theorem 22.3. Evidently these are all elements of K. If we have

$$a_0 + a_1\overline{X} + \cdots a_{n-1}\overline{X}^{n-1} = b_0 + b_1\overline{X} + \cdots b_{n-1}\overline{X}^{n-1}$$

then, by definition, we have

$$(a_0 - b_0) + (a_1 - b_1)X + \cdots + (a_{n-1} - b_{n-1})X^{n-1} \in (f(X)).$$

Since f is of degree n, this is only possible if this is the zero polynomial, i.e. if all the a_i are equal to the corresponding b_i.

Finally, we must prove that any element of K can be written in such a fashion. Write ϕ for the quotient homomorphism $F[X] \to F[X]/(f(X))$. Given any $\alpha \in K$, choose any polynomial g such that $\phi(g) = \alpha$. By the division algorithm, we can write $g = fq + r$ for $f, r \in F[X]$ with $r = 0$ or $\deg(r) < n$.We have that $\phi(g) = \phi(r)$. Writing r as a polynomial of degree less than n (or the zero polynomial), $\phi(r)$ is just the same polynomial with each X replaced by $\overline{X}$; i.e., it is a polynomial of the form given in the question.

20.10. (a). Consider the ideal

$$I = \{af + bg \mid a, b \in F[x]\}.$$

By Theorem 20.1, $I = (h)$ for some polynomial $h \in F[x]$. In particular $h \mid f$ and $h \mid g$ (since $f = 1 \cdot f + 0 \cdot g$ and similarly g are in I). Moreover, if k divides both f and g in $F[x]$, then any k divides any $F[x]$-linear combination of f and g and in particular h. This is what is required to be proved.

(b). Suppose that h_1 and h_2 are two gcd's of f and g. By property (ii) we have $h_1 \mid h_2$ and $h_2 \mid h_1$ so that $h_2 = uh_1$ for some unit $u \in F[x]$, i.e., a nonzero constant.

20.11. We omit the 'only if' part and prove the 'if' part here. Suppose $f(x)$ has a nontrivial factorization $f = gh$ in $F[x]$. Use Corollary 20.4 to write

$$g(x) = (x - c_1) \cdots (x - c_n)$$

in $K[x]$ for some extension K of F, where $1 \leq n < p$. Write $c = \prod_{i=1}^n c_i$. Note that $c \in F$ because it is plus or minus the last coefficient of $g(x)$, which is in $F[x]$.

Now, each of the c_i is a pth root of a. Therefore, $c^p = a^n$. Because $(p, n) = 1$ we may write $1 = pr + ns$ for some $r, s \in \mathbb{Z}$. Therefore $a = a^{pr+ns} = a^{pr}c^{ps} = (a^r c^s)^p$. Since $a, c \in F$ we have $a^r c^s \in F$, i.e., a has a pth root in F, and so it must be a root of f in F.

22.3. (Summary.) We have $[E : \mathbb{Q}] = 8$. Follow example 1 on p. 235, it's kind of a tedious kludge but not actually hard. I don't know of a slick proof that doesn't use Galois theory.

22.4. We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Now, $\sqrt{1+\sqrt{2}}$ is a root of the polynomial $x^2 - (1+\sqrt{2})$ in $\mathbb{Q}(\sqrt{2})$, so if that is irreducible we will know that $[\mathbb{Q}(\sqrt{1+\sqrt{2}} : \mathbb{Q}] = [\mathbb{Q}(\sqrt{1+\sqrt{2}} : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$.

To prove this, write

$$x^2 - (1+\sqrt{2}) = (x + a + b\sqrt{2})(x + c + d\sqrt{2})$$

for some $a, b, c, d \in \mathbb{Q}$. Foiling, we get $-(1+\sqrt{2}) = (ad + bc)\sqrt{2}$, or $-1 - (1 + ad + bc)\sqrt{2} = 0$; since $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, hence linearly independent, so this can't happen.

22.5 $\frac{1+i}{\sqrt{2}}$ is a root of x^4+1. You can show by the usual Eisenstein and $f(x+1)$ trick that this polynomial is irreducible, hence $[E : \mathbb{Q}] = 4$.