MATH453M Homework Solutions Week 8

Nick Inglis
ninglis@math.purdue.edu

3.3.2 a This is irreducible. Either note that it has no root in $\mathbb{Q}$ (the only possible roots are ± 1 and ± 5), or observe that modulo $f(x) \equiv x^3 + x + 1 \pmod 2$, which is irreducible over $\mathbb{Z}_2$.

3.3.2 b Now $3 \nmid 4$, $3 | \pm 6$, $3 | 12$ and $9 \nmid -12$ so $f(x)$ is irreducible by Eisenstein's Criterion with $p = 3$.

3.3.2 c This time $f(x) = (x + 1)(x^2 + 1)$ is not irreducible.

3.3.3 a Possible rational roots are of the form $x = p/q$ with $p \in \{\pm 1, \pm 2\}$ and $q \in \{1, 3\}$ so $x \in \{\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}\}$. Only $-2/3$ is actually a root of $f(x)$. Indeed $f(x) = (3x + 2)(x^2 + x + 1)$, where the last factor has no real roots.

3.3.3 b Possible rational roots have denominator dividing 2 and numerator 1, so the candidates are $\pm 1, \pm 2$. Of these only 2 is a root of $f(x)$. Indeed $f(x) = (x - 2)(x^4 + x^3 + x^2 + x + 1)$, where the last factor has no real roots.

3.3.4 a The only possible rational roots are ± 1, but $f(1) = 1 - 1 + 4 + 1 = 5$ and $f(-1) = 1 + 1 - 4 + 1 = -1$.

3.3.4 b If $f(a) = 0$ then $(a^4)^2 = a^8 = 54$ so $a^4 = \pm 3\sqrt{6} \notin \mathbb{Q}$, hence $a \notin \mathbb{Q}$.

3.3.6 a Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. By the Remainder Theorem, $x + 1$ divides $f(x)$ if and only if $0 = f(1) = a_n + a_{n-1} + \cdots + a_1 + a_0$. Any non-zero coefficients are 1 in $\mathbb{Z}_2$, so this holds if and only if the number of non-zero coefficients is even.

3.3.6 b An irreducible polynomial of degree n will be monic with $0 \neq f(0) = a_)$, so by (a) it will be of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1$, where an odd number of $a_1, a_2, \ldots, a_{n-1}$ are non-zero. For $n \leqslant 3$ any such polynomial is irreducible, so the only irreducible polynomial of degree 2 is $x^2 + x + 1$ and the only two of degree 3 are $x^3 + x + 1$ and $x^3 + x^2 + 1$. For $n = 4$, such a polynomial is irreducible as long as it is not a product of two quadratic irreducibles. therefore $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ is not irreducible, but $x^4 + x + 1$, $x^4 + x^3 + 1$ and $x^4 + x^3 + x^2 + x + 1$ are irreducible. For $n = 5$ we need to avoid products of $x^2 + x + 1$ and a cubic irreducible. This eliminates $x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$ and $x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$. Therefore the irreducibles of degree 5 are

$$x^5 + x^2 + 1, x^5 + x^3 + 1, x^5 + x^3 + x^2 + x + 1, x^5 + x^4 + x^2 + x + 1, x^5 + x^4 + x^3 + x + 1 \text{ and } x^5 + x^4 + x^3 + x^2 + 1.$$

3.3.7 Let $y = x - 1$ so that $x = y = 1$. Now $f(x) = (x^p - 1)/(x - 1)$ so

$$
\begin{aligned}
f(y+1) = \frac{(y+1)^p - 1}{y} &= \frac{y^p + \binom{p}{p-1} y^{p-1} + \cdots + \binom{p}{1} y + 1 - 1}{y} \\
&= y^{p-1} + p y^{p-1} + \cdots + \frac{p(p-1)}{2} y + p.
\end{aligned}
$$

The coefficient of y^i is $\binom{p}{i+1}$ for $0 \leqslant i < p - 1$ and each of these is divisible by p. But the constant coefficient is not divisible by p, so $f(x) = f(y+1)$ is irreducible by Eisenstein's Criterion.

3.3.8 a Let $f(x) = x^p - x$. By Fermat's Little Theorem, $f(n) \equiv 0 \pmod{p}$ for all $n \in \mathbb{Z}$, so every element of $\mathbb{Z}_p$ is a root of $f(x)$.

3.3.8 b Let $g(x) = x^{p-1} - 1 = (x^p - x)/x$ so the non-zero elements of $\mathbb{Z}_p$ are the roots of $g(x)$ and hence the result follows.

3.3.8 c Putting $x = p$ in (b) we see that

$$
(p-1)! = (p-1)(p-2)\ldots(p-(p-1)) \equiv g(p) = p^{p-1} - 1 \equiv -1 \pmod{p}.
$$