Solutions to Homework 8

§3.3 #2. *Decide which of the following polynomials ire irreducible in* $\mathbb{Q}[x]$.

a. x^3+4x^2-3x+5 is irreducible. It has degree 3, so by §3.1 #8 it is enough to show that it has no rational root. By Corollary 3.2, it is enough to check that ± 1 and ± 5 are not roots.

b. $4x^4-6x^2+6x-12$ is irreducible by Eisenstein's criterion with $p=3$.

c. x^3+x^2+x+1 is reducible: -1 is a root.

d. x^4-180 is irreducible by Eisenstein's criterion with $p=5$.

e. $x^4+x^2-6=(x^2+3)(x^2-2)$.

f. $x^4-2x^3+x^2+1$ is irreducible: reducing mod 3 we get $x^4+x^3+x^2+\bar{1}\in \mathbb{Z}_3[x]$, which is in the table of irreducibles on page 112, so the original polynomial is irreducible by Proposition 3.4.

g. $x^3+17x+36$ is irreducible. It has degree 3, so it is enough to show that it has no rational root, but we'd rather not use the rational root test since 36 has so many factors.

   Instead we could reduce mod 5 to get $x^3+\bar{2}x+\bar{1}\in\mathbb{Z}_5[x]$, which has no roots, hence is irreducible, so the original polynomial is irreducible by Proposition 3.4.

h. x^4+x+1 is irreducible: reducing mod 2, we get $x^4+x+\bar{1}\in\mathbb{Z}_2[x]$, and in lecture we saw that this is irreducible, so the original polynomial is irreducible by Proposition 3.4.

i. $x^5+x^3+x^2+1=(x^2+1)(x^3+1)$.

j. x^5+x^3+x+1 is irreducible. We pass to $\mathbb{Z}_3[x]$, where it has no root; thus if it were reducible it would have to be divisible by $x^2+\bar{1}$, $x^2+x+\bar{2}$, or $x^2+\bar{2}x+\bar{2}$ (from the table on page 112), but we do the long division and see that it's not.

If we don't think to reduce mod 3, we can observe that it has no rational root (we only have to check ± 1), so we just have to show that it doesn't factor as

$$(x^2+ax+1)(x^3+bx+c+1) \qquad \text{or} \qquad (x^2+ax-1)(x^3+bx+c-1).$$

In the first case we get

$$a+b=0 \qquad ab+c+1=1 \qquad ac+b+1=0 \qquad a+c=1.$$

Then $b=-a$ and $c=1-a$, so $-a^2-a+2=1$ and $-a^2+1=0$, but latter gives $a=\pm 1$ which contradicts the former. The second case is similar.

The problem that's not from the book.
By the rational root theorem (Proposition 3.1), the polynomial x^2-2 has no roots in $\mathbb{Q}$. Spell out the proof of the theorem in this example. Is it very different from your proof that $\sqrt{2}$ is irrational in §1.2 #11, or is it more or less the same? Explain.

Suppose that r/s were a root of x^2-2, with $\gcd(r,s)=1$. Then $\frac{r^2}{s^2}-2=0$, so $r^2=2s^2$, so $r \mid 2s^2$ and $s \mid r^2$. Because $\gcd(r,s)=1$, this implies that $r \mid 2$ and $s \mid 1$, so $r/s=\pm 1$ or ± 2. But plugging these into x^2-2 we get -1 and 2 respectively, not zero.

My solution to §1.2 #11 took $r^2=2s^2$ and deduced that $2 \mid r^2$, so $2 \mid r$, so $4 \mid r^2=2s^2$, so $2 \mid s^2$, so $2 \mid s$, contradicting the assumption that $\gcd(r,s)=1$. This is superficially similar to the proof above, in that it involves a sequence of deductions about what divides what; but the old proof involves 2 dividing things, and uses the fact that 2 is prime, whereas the new proof involves things dividing 2, and relies on a somewhat more sophisticated statement about dividing a product when you're relatively prime to one of the factors. So upon reflection, I would say that the new proof is *not* just the old one in a different hat, but is really a different proof.

Challenge: §3.3 #10. *Show that $f=x^4-10x^2+1$ is irreducible in $\mathbb{Q}[x]$, yet reducible in $\mathbb{Z}_p[x]$ for every prime p. You may need the following Lemma, whose proof is postponed to Exercise 6.3.33: If neither 2 nor 3 is a square mod p, then 6 is a square mod p.*

We see that f has no rational root, because $f(\pm 1) \neq 0$. So we try to factor it as

$$\begin{aligned} f &= (x^2+ax+b)(x^2+cx+d) \\ &= x^4+(a+b)x^3+(b+ac+d)x^2+(bc+ad)x+bd. \end{aligned}$$

Equating coefficients we see that $a + c = 0$, so $c = -a$, and then

$$\begin{aligned} b - a^2 + d &= -10 \\ a(d - b) &= 0 \\ bd &= 1. \end{aligned}$$

The second equation either gives $a = 0$ or $b = d$.

If $b = d$ then the third equation becomes $b^2 = 1$, so $b = \pm 1$, so the first equation becomes either $a^2 = 12$ or $a^2 = 8$, neither of which has a solution in $\mathbb{Q}$. But if there is an integer m such that $m^2 \equiv 3 \pmod{p}$, then the first one has a solution in $\mathbb{Z}_p$, namely $a = 2\bar{m}$; tracing back through the calculation we get

$$\bar{f} = (x^2 + 2\bar{m}x + 1)(x^2 - 2\bar{m}x + 1) \qquad (\text{where } \bar{m}^2 = \bar{3}).$$

And if there is an n such that $n^2 \equiv 2 \pmod{p}$, then the second one has a solution $\mathbb{Z}_p$, namely $a = 2\bar{n}$; tracing back through the calculation we get

$$\bar{f} = (x^2 + 2\bar{n}x - 1)(x^2 - 2\bar{n}x - 1) \qquad (\text{where } \bar{n}^2 = \bar{2}).$$

If $a = 0$ then the first equation becomes $b + d = 10$ or $d = -b - 10$, so the third equation becomes $-b^2 - 10b = 1$ or $(b+5)^2 = 24$, which has no solution in $\mathbb{Q}$. But if there is an integer k such that $k^2 \equiv 6 \pmod{p}$, then it has a solution in $\mathbb{Z}_p$, namely $b = \bar{2}\bar{k} - \bar{5}$; tracing back through the calculation we get

$$\bar{f} = (x^2 + \bar{2}\bar{k} - \bar{5})(x^2 - \bar{2}\bar{k} - \bar{5}) \qquad (\text{where } \bar{k}^2 = \bar{6}).$$

Thus when we try to factor f as a product of quadratics in $\mathbb{Q}[x]$ then we fail in any case, but if we try to factor $\bar{f}$ in $\mathbb{Z}_p[x]$ then we succeed if either $\bar{2}$ is a square, or $\bar{3}$ is a square, or $\bar{6}$ is a square; and Shifrin gives us a lemma saying that for every p, at least one of these is the case.

Shifrin gives a hint about writing f as a different squares, and I finally figured out what he means. We can write

$$\begin{aligned} f &= (x^2 + 1)^2 - 12x^2 \\ &= (x^2 - 1)^2 - 8x^2 \\ &= (x^2 - 5)^2 - 24. \end{aligned}$$

If $\bar{m}^2 = \bar{3}$ in $\mathbb{Z}_p$ then the first can be factored as $A^2 - B^2 = (A + B)(A - B)$, where $A = x^2 + 1$ and $B = 2\bar{m}x$, giving the first factorization of $\bar{f}$ above. Similarly, if $\bar{2}$ is a square then the second gives the second factorization of $\bar{f}$ above, and if $\bar{6}$ is a square then the third gives the third factorization above.