KMB, 21/10/13

M3P11 Galois Theory, Solutions to problem Sheet 1

1. $K[x]$ is easily checked to be an abelian group under $+$ (the group laws are all easy consequences of the fact that $(K,+)$ is an abelian $f \times 1 = 1 \times f = f$. The reason $(fg)h = f(gh)$ is that if $f = \sum_i a_i x^i$ and $g = \sum_j b_j x^j$ and $h = \sum_k c_k x^k$ then the coefficient of x^ℓ in both $(fg)h$ and $f(gh)$ is $\sum_{i+j+k=\ell} a_i b_j c_k$. Finally distributivity follows because $\sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k}(a_i b_j + a_i c_j)$. Note that we never used inverses so in fact we've proved that if R is a commutative ring with a 1 then so is $R[x]$.

2.

(a) We know 0 is the additive identity in R so $0+0=0$. Hence $0x = (0+0)x = 0x+0x$ and cancelling $0x$ we deduce $0 = 0x$.

(b) If $a \neq 0$ and $b \neq 0$ then there exist multiplicative inverses a^{-1} and b^{-1}, and now $abb^{-1}a^{-1} = 1 \times 1 = 1$. However if $ab = 0$ then we deduce $0(b^{-1}a^{-1}) = 1$ which contradicts part (a) (as $0 \neq 1$ in a field).

(c) Look at top degree terms.

(d) $fh = gh$ implies $(f-g)h = 0$, and if $h \neq 0$ we must have $f - g = 0$ by (c).

3.

(a) Doing long division like in lectures we see $x^5 + x + 1 = (x^3 - x)(x^2 + 1) + 2x + 1$ so the quotient is $x^3 - x$ and the remainder is $2x + 1$.

(b) If $x^{1000}+32x^{53}+8 = q(x)(x-1)+r(x)$ then either $r(x) = 0$ or $\deg(r) < \deg(x-1) = 1$ so in either case r is a constant. Evaluating the equation at $x = 1$ shows us that $r(x) = 1 + 32 + 8 = 41$.

(c) I didn't do an example of this in lectures so I'll do it here.

$$\begin{aligned} 2x^3 + 2x^2 + 3x + 2 &= (2x+2)(x^2+1) + x \\ x^2 + 1 &= (x)(x) + 1 \\ x &= x.1 + 0 \end{aligned}$$

so the last non-zero remainder is 1. Now working backwards,

$$\begin{aligned} 1 &= (x^2+1) - (x).(x) \\ &= (x^2+1) - x.(2x^3 + 2x^2 + 3x + 2 - (2x+2)(x^2+1)) \\ &= (2x^2 + 2x + 1)(x^2+1) - x.(2x^3 + 2x^2 + 3x + 2) \end{aligned}$$

so, if I got it right, one possibility is $s(x) = -x$ and $t(x) = 2x^2 + 2x + 1$. If you got another solution it doesn't mean you are wrong, because there is more than one answer to this sort of question just as in the case of usual integers – for example, you can add $x^2 + 1$ to s and subtract $2x^3 + 2x^2 + 3x + 2$ from t and get a new solution that still works (another bonus question: what's the most general solution? Can you prove it?).

Bonus part: I knew they were coprime in $\mathbb{Q}[x]$ because they're coprime in the bigger ring $\mathbb{C}[x]$ – it's easy to check this because the roots of $x^2 + 1$ are $\pm i$ and neither of these is a root of $2x^3 + 2x^2 + 3x + 2$, as you can see by substituting in.

(d) Euclid again:

$$\begin{aligned} x^4 + 4 &= x(x^3 - 2x + 4) + 2x^2 - 4x + 4 \\ x^3 - 2x + 4 &= (x/2 + 1)(2x^2 - 4x + 4) + 0 \end{aligned}$$

and after that mercifully short procedure we see that the last non-zero remainder is $2x^2 - 4x + 4$. Now hcf's don't really care about constants (see Q4), so $x^2 - 2x + 2$ is another hcf which is kind of nicer (in my opinion), but let's work with what we have and go backwards:

$$2x^2 - 4x + 4 = (x^4 + 4) - x(x^3 - 2x + 4)$$

oh and that's it isn't it – there are serious advantages to Euclid only taking 2 steps! So $a(x) = 1$ and $b(x) = -x$. Actually I see now that the "nicer" hcf wasn't perhaps so nice because then we would have had fractions in a and b.

4. By definition $s \mid t$ and $t \mid s$, so using Q2(c) we deduce that the degrees of s and t must be equal, and $s = tr$ for a polynomial r of degree 0, that is, a non-zero constant. Done!

5. You do these questions by imagining that you're doing long division and seeing what happens. Formal proofs would involve setting up a whole bunch of variable names and would be tedious to write down in full.

(a) Argue like this: $f \mid g$ in $L[x]$ so now use long division to figure out $q(x)$ such that $g(x) = f(x)q(x)$ and now prove by induction on the coefficients of q that all of them are in K (because they are messy combinations of the coefficients of f and g, which are in K).

(b) First part no, e.g. $2x + 2 \mid x + 1$ in $\mathbb{Q}[x]$. Second part yes, and again prove it by figuring out $q(x)$ such that $g(x) = f(x)q(x)$ by long division and noting that you only ever have to divide by 1 when figuring out the coefficients of g.

6.

(i) Spot root $x = 2$; so $x^3 - 8 = (x - 2)(x^2 + 2x + 4)$ and roots of the quadratic are non-real and hence non-rational, so the quadratic must be irreducible (as any factors would be linear).

(ii) Irreducible by Eisenstein ($p = 2$ or $p = 3$).

(iii) In Q3(d) we spotted the factor $x^2 - 2x + 2$, and dividing out we see $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$. Easy check now that both quadratics have non-real and hence non-rational roots, so must be irreducible.

(iv) Eew. Either this is irreducible over $\mathbb{Q}$, or there is a root in $\mathbb{Q}$ (because any factorization must involve a linear term). So let's substitute in $x = p/q$ in lowest terms (i.e. $\gcd(p, q) = 1$) and see what happens. Clearing denominators we get

$$2p^3 + 5p^2q + 5pq^2 + 3q^3 = 0.$$

Now p divides the first three terms of the left hand side, so must divide the fourth which is $3q^3$. But p and q are coprime! So p must divide 3. A similar argument shows that q must divide 2. So $p = \pm 1$ or ± 3 and $q = \pm 1$ or ± 2. Clearly no positive rational is a root (as all the coefficients are positive) so we are left with the possibilities $x = -1, -1/2, -3, -3/2$ and we just try all of them. Miraculously $x = -3/2$ does work! Pulling off the corresponding linear factor gives

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

and the quadratic term has no real roots and hence no rational ones, so this is the factorization into irreducibles.

(v) This one is irreducible by Eisenstein with $p = 3$.

(vi) There's an obvious factor of $x - 1$ and the other factor $x^{72} + x^{71} + \cdots + x + 1$ is irreducible by the trick in lectures after Eisenstein (substitute $y = x - 1$), as 73 is prime.

(vii) This polynomial is obtainable from the polynomial in part (vi): start with the part (vi) polynomial, change x to $-x$ and then change the sign of the polynomial. These sorts of things do not affect things like irreducibility and factorization, so the factorization will be $(x + 1)(x^{72} - x^{71} + \ldots - x + 1)$ and the degree 72 polynomial will be irreducible. Alternatively just find a variant of the trick in lectures ($x = y - 1$ and use Eisenstein).

(viii) Spot roots $x = 1$ and $x = -1$. Over the complexes we have more roots too, like $\pm i$ and so on – how do these control factorization over the rationals? Well $(x - i)$ and $(x + i)$ are factors over the complexes, so their product $x^2 + 1$ is a factor over the complexes and hence also over the rationals (by Q5(a) if you like). Similarly the two complex cube roots of 1 are complex conjugates and are the two roots of $x^2 + x + 1$, and the two 6th roots of 1 that we haven't mentioned yet ($e^{2\pi i/6}$ and its complex conjugate) are roots of $x^2 - x + 1$. So we've just spotted factors whose degrees add up to 8. Let's see what we

have so far then: the factors we have spotted are

$$\begin{aligned}&(x+1)(x-1)(x^2+1)(x^2+x+1)(x^2-x+1)\\&=(x^2-1)(x^2+1)(x^2+x+1)(x^2-x+1)\\&=(x^4-1)(x^4+x^2+1)\end{aligned}$$

and so what is left is

$$\begin{aligned}&(x^{12}-1)/(x^4-1)(x^4+x^2+1)\\&=(x^8+x^4+1)/(x^4+x^2+1)\\&=x^4-x^2+1\end{aligned}$$

The hardest part of this question is figuring out whether that last polynomial factors. If $\zeta = e^{2\pi i/12}$ is a 12th root of unity then the four roots of $x^4 - x^2 + 1$ must be ζ, ζ^5, ζ^7, ζ^{11}, because these are the only four roots which we haven't factored out yet in the above process. None of these roots are rational (because none are real) so $x^4 - x^2 + 1$ has no linear factors over $\mathbb{Q}$. So either $x^4 - x^2 + 1$ is irreducible, or factors into two irreducible quadratic polynomials over $\mathbb{Q}$. These quadratic polynomials will have to have complex conjugate roots, so we are left with the problem of deciding whether $(x - \zeta)(x - \zeta^{11})$ has rational coefficients or not. But, using $\zeta = \cos(2\pi/12) + i\sin(2\pi/12)$ we see that the linear term in this quadratic polynomial is $2\cos(2\pi/12)$ and we all remember from school that $\cos(30^o) = \sqrt{3}/2$ (draw an equilateral triangle; drop a perpendicular; use Pythagoras' theorem!) Hence the quartic really must be irreducible.

An alternative argument for $x^4 - x^2 + 1$: if it were reducible over $\mathbb{Q}$ then it would have to factor into two quadratic polynomials, as before, and by the argument in Gauss' lemma it would have to factor into two quadratic polynomials over $\mathbb{Z}$ too. Looking at top degree and bottom degree terms, this factorization must either be of the form

$$x^4 - x^2 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$$

or

$$x^4 - x^2 + 1 = (x^2 + ax - 1)(x^2 + bx - 1)$$

with a and b integers. Comparing linear terms we get $a + b = 0$ so $b = -a$; now comparing degree 2 terms we get $a^2 = 3$ in the first case and $a^2 = -1$ in the second case, and neither of these have integer solutions, so again we're home.

That one was tougher than I meant it to be – apologies. Still, it's all good for the soul.