GALOIS THEORY
Solutions to Worksheet 1

A 1. (a) Doing long division 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 $X^{2019}+32X^{53}+8=q(X)(X-1)+r(X)$ 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)

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

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 question: what's the most general solution? Can you prove it?).

I knew they were coprime in $\mathbb{Q}[X]$ because they have no roots in common 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. Can you see why this is enough?

(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, 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.

(e) Just one long division gives:

$$-\frac{1}{3}(X^3-2)+\frac{X^2-X+1}{3}(X+1)=1$$

A 2. (a) The previous question, part (e), suggests that we take $a = 1/3$, $b = -1/3$, $c = 1/3$.

(b) The matrix of multiplication by $A + B\xi + \xi^2$ in the basis $1, \xi, \xi^2$ is:

$$T = \begin{pmatrix} A & 2 & 2B \\ B & A & 2 \\ 1 & B & A \end{pmatrix}$$

We find a, b, c by solving the system:

$$T\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

The Cramer rule gives, setting

$$D = \det T = A^3 + 2B^3 - 6AB + 4,$$

the expressions:

$$a = \frac{A^2-2B}{D}, \quad b = \frac{-AB+2}{D}, \quad c = \frac{B^2-A}{D}$$

(What does $D = 0$ mean?)

A 3. The hcf has the property that all other common divisors divide it. So by definition $s \mid t$ and $t \mid s$, so looking at top degree terms 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.

A 4. (a) Divide g by f in $K[X]$ and get a quotient and a remainder, and then pretend eveything is in $L[X]$ and use uniqueness of quotient and remainder to do this part immediately.

(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.