MA 3419: Galois theory

Selected answers/solutions to the assignment due October 17, 2017

1. (**a**) The polynomial $x^2 - x$ works, as it has roots $0, 1, 3, 4$.

(**b**) Suppose that the polynomial $x^2 + ax + b$ has three distinct roots in $\mathbb{Z}/4\mathbb{Z}$. Replacing x by $y = x - u$ and expanding as a polynomial in y, we may assume, without loss of generality, that one of the roots is 0, so that our polynomial is $x^2 + ax = x(x + a)$. Suppose that this polynomial has a root b different from 0 and $-a$ modulo 4. If $b(b + a)$ vanishes in $\mathbb{Z}/4\mathbb{Z}$, and $b \neq 0, -a$, then each of the elements b and $b + a$ must be an even nonzero element of $\mathbb{Z}/4\mathbb{Z}$, so $b = b + a = 2$. This implies $a = 0$, so our polynomial is x^2, which only has one root 0, a contradiction.

2. (**a**) This polynomial does not have roots in $\mathbb{F}_3$ (since $0^2 = 0$, $1^2 = 2^2 = 1$ in $\mathbb{F}_3$), hence irreducible (it is of degree two, so a proper factor is a polynomial of degree one that therefore has a root). The quotient $\mathbb{F}_3[x]/(x^2 + 1)$ is therefore a field; it is a vector space of dimension two over $\mathbb{F}_3$, and so consists of 9 elements. The representatives of cosets are elements $a + bx$ with $a, b \in \mathbb{F}_3$. In the quotient, if we denote the coset of x by i, we have $i^2 + 1 = 0$, so we indeed have the product rule

$$(a + bi)(c + di) = ac - bd + (ad + bc)i.$$

(**b**) The group $(\mathbb{F}_9)^\times$ is cyclic, therefore it is isomorphic to $\mathbb{Z}/8\mathbb{Z}$. In $\mathbb{Z}/8\mathbb{Z}$, exactly four elements can be taken as generators, the cosets of 1, 3, 5, and 7, which are precisely the odd elements, or, multiplicatively, elements that are not squares. We have $(\pm 1)^2 = 1$, $(\pm i)^2 = -1$, $(\pm(1 + i))^2 = 2i = -i$, $(\pm(1 - i))^2 = -2i = i$. Thus, the elements that are not squares are $\pm 1 \pm i$.

3. (**a**) Degree 1: x and $x + 1$. Degree 2: $x^2 + x + 1$ (the others x^2, $x^2 + x = x(x + 1)$ and $x^2+1 = (x+1)^2$ are clearly reducible, and this one clearly has no roots). Degree 3: reducibility for degree 3 is still equivalent to having a root, so we just need to avoid the polynomials with root 0 (constant term 0) and root 1 (sum of coefficients zero). We obtain the polynomials $x^3 + x + 1$ and $x^3 + x^2 + 1$. Degree 4: a reducible polynomial of degree 4 either has a root, or is a product of two irreducibles of degree 2, which we already know. This gives the polynomials $x^4 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$.

(**b**) The rings $\mathbb{F}_2[x]/(x^3 + x + 1)$ and $\mathbb{F}_2[x]/(x^4 + x + 1)$ are fields of $8 = 2^3$ and $16 = 2^4$ elements respectively.

4. (**a**) Suppose that $x^3 + x + 1$ is reducible in $\mathbb{Q}[x]$. Since it is a cubic polynomial, it must have a rational root p/q, where $\gcd(p, q) = 1$. We have $\left(\frac{p}{q}\right)^3 + \frac{p}{q} + 1 = 0$, or, clearing the denominators, $p^3 + pq^2 + q^3 = 0$, so $p^3 = -q^2(p + q)$ and $q^3 = -p(p^2 + q^2)$, which shows that p^3 is divisible by q and q^3 is divisible by p. Since $\gcd(p, q) = 1$, this is possible only for $p = q = \pm 1$, so ± 1 is a root of this polynomial which is clearly false.

Recall from class that to find $1/q(a)$ in $k[x]/(f(x))$, where a is the coset of x, we should find polynomials $r(x)$ and $s(x)$ for which $r(x)f(x) + s(x)q(x) = 1$; then $s(a) = 1/q(a)$.

(**b**) We have $(x^3 + x + 1) - (x^2 + 1)x = 1$, so $1/a = -a^2 - 1$.

(**c**) We have $-(x^3 + x + 1) + (x + 1)(x^2 - x + 2) = 1$, so $1/(a + 1) = a^2 - a + 2$.

(**d**) We have $(x^3 + x + 1) - x(x^2 + 1) = 1$, so $1/(a^2 + 1) = -a$.

5. (**a**) Assume the contrary, so that $\sqrt{3} = a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. This implies $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, so, since $\sqrt{2} \notin \mathbb{Q}$, we have $ab = 0$. If $a = 0$, we have $\sqrt{3} = b\sqrt{2}$, so $\sqrt{\frac{3}{2}}$ is rational, and if $b = 0$, we have $\sqrt{3} = a$ is rational, a contradiction.

(**b**) It is the polynomial $(x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}+\sqrt{3}) = x^4-10x^2+1$. Note that the minimal polynomial of $\sqrt{2}+\sqrt{3}$ must divide this one, so it is sufficient to show that $x^4 - 10x^2 + 1$ is irreducible. The roots of this polynomial are not rational, since if, e.g., $\sqrt{2}+\sqrt{3}$ is rational, then $1/(\sqrt{2}+\sqrt{3}) = \sqrt{3}-\sqrt{2}$ is rational, and consequently $\sqrt{2}$ is rational. Thus, if this polynomial factorises, it is a product of two quadratic polynomial with integer coefficients, $x^4 - 10x^2 + 1 = f(x)g(x)$. The sum of roots of $f(x)$, which is, up to a sign, one of its coefficients, is obtained by adding two of the roots of $x^4 - 10x^2 + 1$; the possible values of this sum is 0, $-2\sqrt{2}$, $2\sqrt{2}$, $-2\sqrt{3}$, $2\sqrt{3}$. Hence, for the coefficients of $f(x)$ to be integers, that sum must be zero, so, without loss of generality, $\sqrt{2} + \sqrt{3}$ and $-\sqrt{2} - \sqrt{3}$ are roots of $f(x)$, and $\sqrt{2} - \sqrt{3}$ and $-\sqrt{2} + \sqrt{3}$ are roots of $g(x)$. But then the product of the roots of $f(x)$ is $-5 + 2\sqrt{6}$ which is not an integer.

(**c**) It is the polynomial $(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3}) = x^2 - 2\sqrt{2}x - 1$. It is irreducible because if it were decomposed as a product of two proper factors, we would have $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

6. Let us prove the result for $a + b$; the proof for ab is completely analogous. Suppose that $f(x)$ and $g(x)$ are the minimal polynomials for a and b over $\mathbb{Q}$. Suppose further that $a_1 = a$, a_2, $\ldots$, a_n and $b_1 = b$, $\ldots$, b_m are, respectively, all roots of those polynomials. Consider the polynomial

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(x - s_i - t_j).$$

The coefficients of this polynomial are polynomial expressions of $s_1, \ldots, s_n$ and $t_1, \ldots, t_m$ with rational coefficients. Since they are invariant under all permutations of $s_1, \ldots, s_n$, they are in $R[e_1, \ldots, e_n]$, where $R = \mathbb{Q}[t_1, \ldots, t_m]$ and e_i are elementary symmetric polynomials of $s_1, \ldots, s_n$. Substituting $s_i = a_i$, we obtain polynomial expressions in $t_1, \ldots, t_m$ with rational coefficients. These are invariant under all permutations of $t_1, \ldots, t_m$, so they are in $\mathbb{Q}[f_1, \ldots, f_m]$, where f_i are elementary symmetric polynomials of $t_1, \ldots, t_m$. Substituting $t_i = b_i$, we obtain rational numbers. Thus the polynomial

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(x - a_i - b_j)$$

with one of the roots $a_1 + b_1 = a + b$ has rational coefficients, which completes the proof.