Algebra 2 Homework 6

March 15, 2024

Solution of problem 1:

1. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where a_i is the coefficient of the term of degree i, and $a_n \neq 0$. See that the reverse of this polynomial will have degree n, Since $x^n f(1/x) = x^n \left(a_0 + a_1x^{-1} + \cdots + a_nx^{-n}\right)$
2. Let the constant coefficient and leading term both be non-zero (If not, then one could have $x^2 + x$, which is reducible, while its reverse, $x + 1$ is irreducible). It is easy to see that the reverse of the reverse is just the original polynomial. That is, $x^n(x^{-n}f(x)) = f(x)$. Thus we only need to show that if f is reducible, g is reducible. If $f(x) = p(x)q(x)$, where p, q are not units, and $d_p := \deg p(x) > 1$ and $d_q := \deg q(x) > 1$. Since the constant term of f is non-zero, the constant term of p and q must also be non-zero. Replacing x by $\frac{1}{x}$, and multiplying on both sides by x^n, we get
$$x^n f\left(\frac{1}{x}\right) = x^{d_p} p\left(\frac{1}{x}\right) \cdot x^{d_q} q\left(\frac{1}{x}\right) = \ell(x)m(x),$$
which gives us a factorisation for the reverse of f.

□

Solution of problem 2: We begin by enumerating all irreducible polynomials of degree $1, 2$ and 4. See that x and $x+1$, the only degree one polynomials, are irreducible. For degree 2, we have four choices. Of these, x^2, x^2+x and x^2+1 are reducible. x^2+x+1 is irreducible since it has no roots, plugging in 0 and 1. For degree 4, we have sixteen choices. Of these, we must weed out the reducible polynomials. We can also calculate the irreducibles of degree 3 easily, since we can use them to find the reducible polynomials of degree 4. We have eight possibilities for polynomials of degree four, we can eliminate six of them easily, with a mixture of clever thinking and brute force ($x^3, x^3+1, x^3+x^2+x+1, x^3+x, x^3+x^2, x^3+x^2+x$ are reducible) we can see that x^3+x+1 and x^3+x^2+1 are irreducible. A clever trick that shall aid us in our effort to weed out reducible polynomials is to notice that if there is a polynomial which has evenly many non-zero terms, than it must be reducible since then we have $1+\cdots+1$ even number of times. Therefore an irreducible polynomial must necessarily have odd number of terms with constant term 1. This gives us $x^4+x^3+x^2+x+1, x^4+x^3+1, x^4+x^2+1$, and x^4+x+1. In the case of x^4+x^2+1, see that it is $(x^2+x+1)^2$, so this must be excluded. Thus we only have three irreducible polynomials in $\mathbb{F}_2[x]$ of degree 4. The polynomials all have 16 distinct roots, and 15 non-zero roots. The only possibility in $\mathbb{F}_2[x]$ is $x^{15}-1$. Multiplying by x, we have $x^{16}-x$, which is the required polynomial. □

Solution of problem 3: See that $f(x+1)-f(x) = (x+1)^p-(x+1)+a-x^p+x-a = 1-1 = 0$. Thus either the polynomial has a root for all $x \in \mathbb{F}_p$, or it has no roots in $\mathbb{F}_p$. Assuming it has a root, then we must have that 0 is also a root, which forces $a = 0$, which is not possible. Thus f has no linear factors. Now see that $F_p(\alpha) = F_p(\alpha')$, where α, α' are two roots of the polynomial, both of whom are not in $\mathbb{F}_p$. Then their irreducible polynomials must be equal, which must divide f. Then the degree of f is some multiple of q, which is the degree of α. However, since p is prime, q is either 1 or p. Since the first is not possible, the polynomial must be irreducible.

We see that $f'(x) = -1$. Then the gcd can only be a constant, which means that there can be no common root between f and f'. Thus this polynomial is separable. $\square$

Solution of problem 4*:* Let L be an extension of K that contains all the roots of $f(x)$. If $f(x)$ had repeated irreducible factors in $K[x]$, there would be multiple roots of $f(x)$ in L. However, since L is also an extension of F, it contradicts the separability of $f(x)$ over F, which is a contradiction. Thus $f(x)$ cannot have repeated irreducible factors in $K[x]$. $\square$

Solution of problem 5*:* If we had an isomorphism $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$, then we consider the map

$$\begin{tikzcd} & \mathbb{Q}[x] \arrow[dl, two heads, "x\mapsto\sqrt{2}"'] \arrow[dr, two heads, "x\mapsto\sqrt{3}"] & \\ \mathbb{Q}(\sqrt{2}) \arrow[rr, dash, "f"] & & \mathbb{Q}(\sqrt{3}) \end{tikzcd}$$

This map must commute, so $x \mapsto \sqrt{2} \mapsto f(\sqrt{2})$. But since the above diagram must commute, we have $f(\sqrt{2}) = \sqrt{3}$. (It does not matter if we send $\sqrt{2}$ to $\sqrt{3}$ or its conjugate, the end result is the same). If $f(\sqrt{2}) = \sqrt{3}$, then we have $2 = f(2) = f(\sqrt{2}\cdot\sqrt{2}) = f(\sqrt{2})f(\sqrt{2})\sqrt{3}\cdot\sqrt{3} = 3$. This means that

$$2 = 3 \implies 2 - 3 = 0 \implies -1 = 0 \implies -1 \cdot -1 = -1 \cdot 0 \implies 1 = 0,$$

which is known to be not possible. Thus the two fields do not exist.

$\square$

Solution of problem 6*:*

1. We need to check that this is a homomorphism that is one-one and onto. Note that k is not affected, since the mapping affects only x. Then is map is $k-$linear. Thus acting on the vector space of all polynomials on k, this is clearly a linear map. To see that it respect the ring operation as well, we want to see that $\varphi(x^m \cdot x^n) = \varphi(x^m)\varphi(x^n)$. The two sides are clearly equal, so we can extend this to all polynomials, claiming that $\varphi(f(t) \cdot g(t)) = \varphi(f(t)) \cdot \varphi(g(t))$. See that the degree of $\varphi(f(t))$ is the same as the degree of $f(t)$, since for each monomial the degree is preserved. Now see that the kernel must be trivial, since we say that 0 has an undefined degree and it is the only such element. Thus any polynomial that goes to 0 under φ must also have that same degree, which means that our map is onto. To see that our map is onto, we propose that the map $\tau(f(x)) := f\left(\frac{x-b}{a}\right)$, which is the inverse of φ. Since a is non-zero, it is invertible. Since this is also a map just like φ, we see that this also has all of the properties of φ. Now see that $\tau(\varphi(f(t))) = \tau(f(at+b)) = \tau\left(\frac{at+b-b}{a}\right) = f(t)$, and $\varphi(\tau(f(t))) = \varphi\left(f\left(\frac{t-b}{a}\right)\right) = f\left(a\frac{t-b}{a} + b\right) = f(t)$. Thus φ is onto, and hence an automorphism.

2. We have φ, an automorphism on $k[t]$. We only need to know where t is sent. Let $x \mapsto p(t)$. If $p(t)$ is constant, it is not an automorphism. Let the inverse map be such that $x \mapsto g(t)$. Then $f(g(t)) = t$. This implies that $\deg f \cdot \deg g = 1 \implies \deg f = \deg g = 1$. Then $f(t) = at + b$, a linear polynomial ($a \neq 0$).

$\square$

Solution of problem 7: 1. Fix a $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. Then for some number $k^2 \in \mathbb{R}$, we have $\sigma(k^2) = \sigma(k)^2$. Therefore square numbers are taken to square numbers. If $r > 0$, then $r = k^2$, for some $k \in \mathbb{R}$, then we have the squares are taken to squares and hence $\sigma(r) = \sigma(k^2) = \sigma(k)^2 > 0$.
Now see that if $a < b$, $b - a > 0$. Thus $\sigma(b - a) > 0$, that is $\sigma(b) > \sigma(a)$.

2. If $\frac{-1}{m} < a - b < \frac{1}{m}$, then applying σ yields $\frac{-1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$. The bounds are unchanged since the automorphism is identity over the rationals. Pick any $\varepsilon > 0$. Then if we want $|\sigma(b - a)| < \varepsilon$, we just find the least $N(\varepsilon) \in \mathbb{N}$ such that $\frac{1}{N(\varepsilon)} < \varepsilon$. Then let $\delta = \frac{1}{N(\varepsilon)}$, which means all automorphisms are continuous.
3. We know that σ is the identity on the rationals, which is a dense subset of $\mathbb{R}$. Pick a sequence $\{q_n\}$ such that $q_n \to r$ as $n \to \infty$. Then by continuity of σ we have $\sigma(q_n) \to \sigma(r)$. The sequence $\{\sigma(q_n)\}$ is just the sequence $\{q_n\}$, which can only converge to r. Since limits are unique in $\mathbb{R}$, we have $\sigma(r) = r$. Thus σ is the identity on $\mathbb{R}$. Since our choice of σ was arbitrary, we have that $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 0$.

$\square$