Math 5055: Advanced Algebra II

Assignment 1

Solutions

1. **Show that x^3+9x+6 is irreducible over $\mathbb{Q}$. Let θ be a root, and compute $(1+\theta)^{-1} \in \mathbb{Q}[\theta]$.**

   A cubic is irreducible if and only if it has no roots, and a monic polynomial over $\mathbb{Z}$ has a root over $\mathbb{Q}$ if and only if it has a root over $\mathbb{Z}$. So it suffices to check that $x^3 + 9x + 6$ has no integral roots. Well, if $|x| \geq 4$ then $|x^3| > 3x^2 + x^2/2 > |9x| + 8$, so there x cannot be a root of $x^3 + 9x + 6$. This leaves just $x \in \{\pm 3, \pm 2, \pm 1, 0\}$ to check, and indeed there are no integral roots.

   Note that $1, \theta, \theta^2$ is a $\mathbb{Q}$-basis for $\mathbb{Q}[\theta]$, since $\deg \theta = 3$. So we wish to find rational numbers a, b, c such that $1 = (1+\theta)(a+b\theta+c\theta^2) = a + (a+b)\theta + (b+c)\theta^2 + c\theta^3$. Since $\theta^3 = -9\theta - 6$, the RHS simplifies to $(a-6c) + (a+b-9c)\theta + (b+c)\theta^2$. So $b = -c$ and $a = 10c$ and $1 = 4c$. Thus we find $\boxed{(1+\theta)^{-1} = \frac{5}{2} - \frac{1}{4}\theta + \frac{1}{4}\theta^2}$.

2. **Show that x^3+x+1 is irreducible over $\mathbb{F}_2$. Let θ be a root, and compute its powers in $\mathbb{F}_2[\theta]$.**

   A cubic is irreducible if and only if it has no roots. It suffices to check just $x = 0, 1$, and: $0^3 + 0 + 1 = 1$ and $1^3 + 1 + 1 = 1$ in $\mathbb{F}_2$.

   In $\mathbb{F}_2[\theta]$, we have $\theta^3 = \theta + 1$. Thus the powers of θ are:

   $$1, \theta, \theta^2, \theta+1, \theta^2+\theta, \theta^2+\theta+1, \theta^2+1, 1, \ldots$$

   whence it repeats. In other words, $\theta^8 = 1$, and all the nonzero elements of $\mathbb{F}_2[\theta]$ are powers of θ.

3. **Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be two finite extensions of a field $\mathbb{F}$, both subextensions of a common extension $\mathbb{E}$; recall that $\mathbb{K}_1\mathbb{K}_2 \subset \mathbb{E}$ is the subextension that they generate. Show that the tensor product algebra $\mathbb{K}_1 \otimes_{\mathbb{F}} \mathbb{K}_2$ is a field if and only if $[\mathbb{K}_1\mathbb{K}_2 : \mathbb{F}] = [\mathbb{K}_1 : \mathbb{F}][\mathbb{K}_2 : \mathbb{F}]$. Conclude that this happens in particular whenever $[\mathbb{K}_1 : \mathbb{F}]$ and $[\mathbb{K}_2 : \mathbb{F}]$ are coprime.**

   Using commutativity, the linear map $\mu : \mathbb{K}_1 \otimes \mathbb{K}_2 \to \mathbb{K}_1\mathbb{K}_2$ defined on pure tensors by $\mu(a_1 \otimes a_2) = a_1 a_2$ is easily seen to be a surjective ring homomorphism. If $\mathbb{K}_1 \otimes_{\mathbb{F}} \mathbb{K}_2$ is a field, then μ must be injective and hence an isomorphism, and if $\mathbb{K}_1 \otimes_{\mathbb{F}} \mathbb{K}_2$ is not a field, then μ must have kernel. On the other hand, since μ is surjective, it does or does not have a kernel depending on whether $\dim_{\mathbb{F}}(\mathbb{K}_1 \otimes_{\mathbb{F}} \mathbb{K}_2)$ is equal to or greater than $\dim_{\mathbb{F}}(\mathbb{K}_1\mathbb{K}_2)$. But tensor products multiply dimensions.

   Since $[\mathbb{K}_1 : \mathbb{F}]$ and $[\mathbb{K}_2 : \mathbb{F}]$ both divide $[\mathbb{K}_1\mathbb{K}_2 : \mathbb{F}]$, if $[\mathbb{K}_1 : \mathbb{F}]$ and $[\mathbb{K}_2 : \mathbb{F}]$ are coprime, then their product divides $[\mathbb{K}_1\mathbb{K}_2 : \mathbb{F}]$, which on the other hand is not more than their product.

4. **In the field $\mathbb{F}(x)$ of rational functions, let $u = x^3/(x+1)$, and consider the subfield $\mathbb{F}(u) \subset \mathbb{F}(x)$. Compute the degree of this field extension.**

   Clearing denominators, we find that $x^3 - ux - u = 0$. In other words, x solves the polynomial $f(x) = x^3 - ux - u \in \mathbb{F}(u)[x]$. We claim that this $f(x)$ is the minimal polynomial of x over $\mathbb{F}(u)$, in which case the extension $\mathbb{F}(u) \subset \mathbb{F}(x)$ has degree 3. This is equivalent to claiming that $f(x) \in \mathbb{F}(u)[x]$ is irreducible. Since $f(x)$ is cubic, to show that it is irreducible, it suffices to check that it has no roots. Suppose for contradiction that $f(v) = 0$ where $v = \frac{a(u)}{b(u)} \in \mathbb{F}(u)$ and $a(u), b(u) \in \mathbb{F}[u]$ are relatively prime. Clearing denominators would give

   $$a^3 - uab^2 - ub^3 = 0.$$

   Thus any prime factor of b is also a prime factor of a^3 and hence of a, and conversely any prime factor of a is also a prime factor of ub^3 and hence of either u or b. Since a and b are assumed relatively prime, we see that $b = 1$ and $a = u^m$ for some $m \in \mathbb{N}$. But u^m is not a root of f.

5. **A field $\mathbb{F}$ is *formally real* if -1 is not a sum of squares in $\mathbb{F}$. Suppose that $\mathbb{F}$ is formally real and that $f(x) \in \mathbb{F}[x]$ is irreducible of odd degree, and pick a root α of $f(x)$. Show that $\mathbb{F}(\alpha)$ is formally real.**

   Let $\deg f = \deg \alpha = n$. Suppose that $\mathbb{F}(\alpha)$ is not formally real, i.e. that $-1 = a^2 + b^2 + \dots$ is a sum of squares in $\mathbb{F}(\alpha)$. What is an element $a \in \mathbb{F}(\alpha)$? It is $a(\alpha)$ for a unique polynomial $a(x) \in \mathbb{F}(x)$ of degree $\deg a < n$. And the equation $-1 = a^2 + b^2 + \dots$ is an equation of polynomials mod $f(x)$. In other words

   $$a(x)^2 + b(x)^2 + \dots = -1 \mod f(x)$$

   or in other words

   $$a(x)^2 + b(x)^2 + \dots = -1 + f(x)g(x)$$

   for some $g(x) \in \mathbb{F}[x]$. Now count degrees: $a, b, \dots$ each have degree $\leq n-1$, and so the LHS has degree $\leq 2n-2$. But the RHS has degree $n + \deg(g)$, and so $\deg(g) \leq n-2$. Moreover, the LHS is even, and so $\deg f$ and $\deg g$ have the same parity.

   But the same equation shows that -1 is a sum of squares in $\mathbb{F}[x]/(g(x))$, and hence in any field quotient thereof.

   We'd like to claim that this leads to an "infinite descent" contradiction, in which we keep reducing the degree. But there is a problem. Specifically, what if $\deg g = 0$? Then $\mathbb{F}[x]/(g(x)) = 0$ is the zero ring, and has no field quotients.

   Ruling this out is where we use the assumption that $\deg f = n$ is odd. Then $\deg g$ is also odd, and so $g(x)$ definitely has an irreducible factor *of odd degree*. So now we see the infinite descent: start with $f = f_0$, find g, and then choose f_1 to be an odd-degree irreducible factor of g; then $\deg f_1 < \deg f_0$ and both are odd, and arrive at the desired contradiction.

6. **Let $\mathbb{E}$ be a finite extension of $\mathbb{F}$. Show that $\mathbb{E}$ is a splitting field (of some set of polynomials) over $\mathbb{F}$ if and only if every irreducible polynomial over $\mathbb{F}$ which admits a root in $\mathbb{E}$ splits completely in $\mathbb{E}$.**

   Let $S \subset \mathbb{F}[x]$ be the set of polyonials for which $\mathbb{E}$ is declared the splitting field. (If this set is finite, then we may as well work with the polynomial $S(x) = \prod_{s \in S} s(x)$.)

Let $f(x) \in \mathbb{F}[x]$ be irreducible, and $\alpha \in \mathbb{E}$ a root of f. In other words, we have field extensions

$$\mathbb{F} \subset \mathbb{F}[\alpha] \subset \mathbb{E}$$

where $\mathbb{F}[\alpha] \cong \mathbb{F}[x]/(f(x))$. Note that the extension $\mathbb{F}[\alpha] \subset \mathbb{E}$ is again a splitting field for the same set S, now thought of as a set of polynomials in $\mathbb{F}[\alpha][x]$. Let $\mathbb{K}$ denote the splitting field for $S \cup \{f\}$. In other words, we have

$$\mathbb{E} \subset \mathbb{K},$$

and f splits completely in $\mathbb{K}$.

Now pick some other root $\beta \in \mathbb{K}$ of f, and inspect the subfield $\mathbb{F}[\beta] \subset \mathbb{K}$. There is a canonical isomorphism $\mathbb{F}[\alpha] \cong \mathbb{F}[\beta]$, namely the unique one which is the identity on $\mathbb{F}$ and takes $\alpha \mapsto \beta$. Let $\mathbb{E}'$ be the splitting field of S over $\mathbb{F}[\beta]$.

Then, from the theorem, we can choose an isomorphism $\mathbb{E} \cong \mathbb{E}'$ taking $\alpha \mapsto \beta$ and acting as the identity on $\mathbb{F}$. In particular, $[\mathbb{E} : \mathbb{F}] = [\mathbb{E}' : \mathbb{F}]$.

On the other hand, $\mathbb{E}$ is a subfield of $\mathbb{E}'$. Indeed, $\mathbb{E}' = \mathbb{E}[\beta]$ (since $\mathbb{E}$ is generated by the roots of the elements of S whereas $\mathbb{E}'$ is generated by those roots together with β). Since we assumed that the index $[\mathbb{E} : \mathbb{F}]$ is finite, we must have $\mathbb{E} = \mathbb{E}'$.

But this means in particular that $\beta \in \mathbb{E}$, which is what we wanted to prove.