SOLUTIONS TO FIELD EXTENSION REVIEW SHEET

MATH 435 SPRING 2011

1. Polynomials and roots

Exercise 1.1. Prove that $\mathbb{Q}[i] = \mathbb{Q}(i)$.

Solution: We need to prove that $\mathbb{Q}[i]$ is a field. So choose $a+bi \in \mathbb{Q}[i]$, with $a+bi \neq 0$. Then $1/(a+bi) = (a-bi)/(a^2+b^2) = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i \in \mathbb{Q}[i]$. As desired.

Exercise 1.2. Now, suppose K is a field, and $p(x) \in K[x]$ is an irreducible polynomial (and non-zero). Prove that $K[x]/\langle p(x)\rangle$ is a field by proving that $\langle p(x)\rangle$ is maximal (use the fact that $K[x]$ is a PID).

Solution: Suppose there exists an ideal $\langle p(x)\rangle \subseteq I \subseteq K[x]$. Because $K[x]$ is a PID, $I = \langle q(x)\rangle$ for some $q(x) \in K[x]$. Thus $p(x) \in \langle q(x)\rangle$. In other words, there exists a $r(x) \in K[x]$ such that $p(x) = r(x)q(x)$. Since $p(x)$ is irreducible, either $r(x)$ or $q(x)$ is a unit. If $r(x)$ is a unit then $q(x) = p(x)\frac{1}{r(x)}$ and so $q(x) \in \langle p(x)\rangle$ proving that $I = \langle p(x)\rangle$. If $q(x)$ is a unit, then $I = K[x]$. Thus we have proven that $\langle p(x)\rangle$ is maximal.

Exercise 1.4. Suppose that $k \subseteq E$ is a field extension and $\alpha \in E$ is a root of an irreducible polynomial $p(x) \in k[x]$. Then prove that

$$k[x]/\langle p(x)\rangle \cong k[\alpha] = k(\alpha).$$

Note you have to prove two statements.

Solution: First consider the map $\phi : k[x] \to k[\alpha]$ which sends $f(x)$ to $f(\alpha)$. This map is clearly surjective and $f(x)$ is in the kernel if and only if $f(\alpha) = 0$. Since $p(\alpha) = 0$, $p(x) \in I = \ker(\phi)$. But $\langle p(x)\rangle$ is maximal, and I is clearly not $k[x]$ (since 1 goes to 1, not zero), thus $I = \langle p(x)\rangle$. By the first isomorphism theorem, $k[x]/I = k[x]/\langle p(x)\rangle \cong k[\alpha]$. This proves the first part.

Now, the left side of that equation is a field and thus $k[\alpha]$ is a field. But $k[\alpha] \subseteq k(\alpha)$ and $k(\alpha)$ is the smallest field containing k and α so $k[\alpha] = k(\alpha)$, proving the second part.

2. Vector spaces

Exercise 2.2. Suppose that $F \subseteq K$ is a field extension. Prove that K is an F-vector-space with the multiplication rule $a.b = ab$ for $a \in F$ and $b \in K$.

Solution: Of course K is already an Abelian group under addition. Now we check the vector space properties. Certainly $1.b = 1b = b$. Likewise $a.(b+c) = a(b+c) = ab + ac = a.b + a.c$ and $(a+a').b = ab + a'b = a.b = a'.b$ and finally $(aa').b = (aa')b = a(a'b) = a(a'.b) = a.(a'.b)$. Thus it is a vector space.

Exercise 2.4. Suppose that K is a field and that $p(x) \in K[x]$ is irreducible. Find a basis for $K[x]/\langle p(x)\rangle$ over K. Prove that the set you found really is a basis.

Solution: Set d to be the degree of $p(x)$ and write $I = \langle p(x)\rangle$ for simplicity. Consider the set $\mathcal{B} = \{1+I, x+I, x^2+I, \ldots, x^{d-1}+I\}$. We prove that this is a spanning set for $K[x]/I$. First choose $g(x)+I$ and write $g(x) = p(x)q(x) + r(x)$ with $\deg r(x) < d$. Then

$g(x) + I = r(x) + I$ and so $g(x)$ is equal to a K-linear combination of the elements in $\mathcal{B}$. This proves that $\mathcal{B}$ is a spanning set.

Now suppose that

$$0 + I = (a_0 1 + I) + (a_1 x + I) + \cdots + (a_{d-1}x^{d-1} + I) = (a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}) + I$$

for some $a_i \in K$. Thus $(a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}) \in I$ (we just need the version for Abelian groups here). But this means that $p(x)$ divides $a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$ which is absurd for degree reasons, unless all the a_i are zero. Thus all the a_i are zero which proves that $\mathcal{B}$ is linearly independent.

3. Extension degree

Exercise 3.2. Prove the following.

(i) $[\mathbb{R} : \mathbb{Q}] = \infty$.
(ii) $[\mathbb{Q}[\sqrt{7}] : \mathbb{Q}] = 2$.
(iii) $[\mathbb{Q}[x]/(x^5 + 5x^2 + 10) : \mathbb{Q}] = 5$.
(iv) If $k \subseteq L$ is a finite extension, and $k \subseteq K \subseteq L$ is a subextension, then $k \subseteq K$ and $K \subseteq L$ are also finite.

Solution:

(i) Certainly $\mathbb{R}$ contains roots of $x^n - 2$ for all integers n. Each of those live in an extension of degree at least n by Exercise 2.4. This means that $[\mathbb{R} : \mathbb{Q}]$ is bigger than any integer.
(ii) $\mathbb{Q}[\sqrt{7}] \cong \mathbb{Q}[x]/\langle x^2 - 7\rangle$ which obviously is a two-dimensional vector space over $\mathbb{Q}$ by Exercise 2.4.
(iii) The polynomial is irreducible by Eisenstein, and so again the result follows by Exercise 2.4.
(iv) Choose a basis $l_1, \ldots, l_n$ for L over k. This serves as a spanning set for L over K and so L's basis over K may have even fewer elements than n (but certainly finite). For K over k, just observe that K is a subspace of a finite dimensional vector space.

One of the main tools for measuring extension degree is as follows:

Exercise 3.4. Use the previous theorem to prove the following.

(i) $\sqrt{3}$ is not contained in $\mathbb{Q}[3^{1/5}]$.
(ii) $\sqrt{3}$ is not contained in $\mathbb{Q}[3^{1/3}, 2^{1/3}]$.
(iii) The 7th root of two is not contained in the splitting field of $x^5 - 2$ over $\mathbb{Q}$.
(iv) If $\mathbb{F}_{p^d}$ is a subset of $\mathbb{F}_{p^n}$ then d divides n.

Solution:

(i) $\sqrt{3}$ can only live in extensions over $\mathbb{Q}$ of even degree by Theorem 3.3. The given extension has degree 5.
(ii) We leave it to you (possibly with the aid of a computer algebra system) to prove that $2^{1/3}$ is not in $\mathbb{Q}[3^{1/3}]$. Consider the polynomial $x^3 - 2$. This polynomial has one real root, $2^{1/3}$ and two complex roots, neither of which are in $\mathbb{Q}[3^{1/3}]$. Thus $x^3 - 2$ is irreducible in $\mathbb{Q}[3^{1/3}]$ and so $\mathbb{Q}[3^{1/3}, 2^{1/3}]$ is a degree $(3)(3) = 9$ extension of $\mathbb{Q}$. But 2 does not divide 9, and so $\sqrt{3}$ cannot be in there.
(iii) One obtains the splitting field by adjoining one root at a time. The degree of the splitting field is of the form $(5)(a)(b)(c)(d)$ where $a \leq 4$, $b \leq 3$, $c \leq 2$ and $d \leq 1$. The prime number 7 cannot divide that product.
(iv) $\mathbb{F}_{p^d}$ is a degree d extension of $\mathbb{F}_p$ (it has p^d different elements). Likewise $\mathbb{F}_{p^n}$ is a degree n extension. Thus d divides n by Theorem 3.3.

4. Algebraic and transcendental elements

Exercise 4.3. Prove that every $x \in k$ is algebraic over k.

Solution: It is a root of the polynomial $z - x \in k[z]$ and thus algebraic.

Exercise 4.7. Suppose that $k \subseteq E$ is an extension field and $\beta \in E$ is transcendental over k. Then $k[\beta] \cong k[x]$, the polynomials in x with coefficients in k.

Solution: Consider the function $\phi : k[x] \to k[\beta]$ defined by $\phi(g(x)) = g(\beta)$.. Certainly this function is surjective. As before, the kernel is all elements $g(x) \in k[x]$ such that $g(\beta) = 0$, but since β is transcendental, there are no such elements except the constant zero. Thus $k[x] \cong k[x]/\langle 0\rangle \cong k[\beta]$ as desired.

5. Splitting fields

Exercise 5.3. Determine whether or not the following extensions are splitting fields.

(i) $\mathbb{F}_3 \subseteq \mathbb{F}_3[x]/\langle x^5 + 1\rangle$ for the polynomial $x^5 + 1 \in \mathbb{F}_3[x]$.
(ii) $\mathbb{Q} \subseteq \mathbb{C}$ for the polynomial $x^2 + 1 \in \mathbb{Q}[x]$.
(iii) $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$ for the polynomial $x^2 - 2$.
(iv) $\mathbb{Q} \subseteq \mathbb{Q}[i5^{1/4}]$ for the polynomial $x^4 - 5$.

Solution:

(i) No. The polynomial x^5+1 is not even irreducible since 2 is a root. Thus $\mathbb{F}_3[x]/\langle x^5 + 1\rangle$ is not a field and this is not a splitting field.
(ii) No. While $x^2 + 1$ certainly splits in $\mathbb{Q}$, $\mathbb{C}$ is certainly not the smallest extension in which $x^2 + 1$ splits, so this is not a splitting field.
(iii) Yes, $x^2 - 2$ factors as $(x - \sqrt{2})(x + \sqrt{2})$ and since the degree of the extension is 2, this must be the smallest such extension.
(iv) No, $i5^{1/4}$ is a root so $\mathbb{Q}[i5^{1/4}] \cong \mathbb{Q}[x]/(x^4 - 5) \cong \mathbb{Q}[5^{1/4}]$. But $\mathbb{Q}[5^{1/4}]$ is not the splitting field since it doesn't contain the root $i5^{1/4}$ (since it is in $\mathbb{R}$). Since $x^4 - 5$ doesn't split in $\mathbb{Q}[5^{1/4}]$, it doesn't split in the isomorphic field $\mathbb{Q}[i5^{1/4}]$ either.

Exercise 5.4. Show that the splitting field for $x^{(p^n)} - x$ over $\mathbb{F}_p$ has exactly p^n elements.

Solution: The solutions to $x^{(p^n)} - x$ form a field as we've shown before in class. There are also no multiple roots by the derivative test, so there are p^n such roots. Therefore the smallest field containing all those roots is exactly the field made up of those p^n elements.