FIELD EXTENSION REVIEW SHEET

MATH 435 SPRING 2011

1. Polynomials and roots

Suppose that k is a field. Then for any element x (possibly in some field extension, possibly an indeterminate), we use

- $k[x]$ to denote the smallest ring containing both k and x.
- $k(x)$ to denote the smallest field containing both k and x.

Given finitely many elements, $x_1, \dots, x_n$, we can also construct $k[x_1, \dots, x_n]$ or $k(x_1, \dots, x_n)$ analogously. Likewise, we can perform similar constructions for infinite collections of elements (which we denote similarly).

Notice that sometimes $\mathbb{Q}[x] = \mathbb{Q}(x)$ depending on what x is. For example:

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

Now, suppose K is a field, and $p(x) \in K[x]$ is an irreducible polynomial. Then $p(x)$ is also prime (since $K[x]$ is a PID) and so $K[x]/\langle p(x)\rangle$ is automatically an integral domain.

Exercise 1.2. 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).

Definition 1.3. An *extension field of* k is another field K such that $k \subseteq K$.

Given an irreducible $p(x) \in K[x]$ we view $K[x]/\langle p(x)\rangle$ as an extension field of k. In particular, one always has an injection $k \to K[x]/\langle p(x)\rangle$ which sends $a \mapsto a + \langle p(x)\rangle$. We then identify k with its image in $K[x]/\langle p(x)\rangle$.

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.

The previous exercise should be viewed as saying that

> $k[x]/\langle p(x)\rangle$ is the smallest field extension of k containing a "generic" root of $p(x)$.

It is very important to note that if α and α' are two roots, then $k[\alpha] \cong k[\alpha']$ because they are both isomorphic to $k[x]/\langle p(x)\rangle$, even though the two extensions might have totally different elements. In particular, it is possible that $\alpha \notin k[\alpha']$ even if α and α' are roots of the same polynomial.

2. Vector spaces

We recall the definition of a vector space over k.

Definition 2.1. A *vector space over* k is an Abelian group V, under addition, with a multiplication rule $a.x \in V$ for $a \in k$ and $x \in V$, satisfying the following axioms for $x, y \in V$ and $a, b \in k$.:

(i) $a.(x + y) = a.x + a.y$

(ii) $(a+b).x = a.x + b.x$
(iii) $(ab).x = a.(b.x)$
(iv) $1.x = x$

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 $b \in K$.

Definition 2.3. If V is a vector space over k, a *basis for V over k* is a set $\{x_1, \ldots, x_n\}$ that is both linearly independent[1] and a spanning set[2]

It is a fact that if V has a finite basis over k, then all other bases are also finite and with the same number of elements. This number of elements in called the *dimension of V over k*. If there is no finite basis, the dimension of V over k is called infinity.

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.

3. Extension degree

Definition 3.1. Suppose that $k \subseteq K$ is a field extension. We define the *degree of K over k*, denoted by $[K : k]$ to be the dimension of K as a k-vector space. It might be that $[K : k] = \infty$. If $[K : k]$ is not infinity, then we say that $k \subseteq K$ is a *finite extension.*

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.

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

Theorem 3.3. *Suppose that $F \subseteq K \subseteq L$ is a sequence of extension fields. Then*
$$[L : F] = [L : K] \cdot [K : F].$$

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.

4. Algebraic and transcendental elements

Definition 4.1. Suppose that $k \subseteq E$ is a field extension and $\alpha \in E$. Then α is called an *algebraic element over k* if there exists a non-constant polynomial $p(x) \in k[x]$ such that $p(\alpha) = 0$. An element is called *transcendental* if it is not algebraic.

Remark 4.2. Sometimes we say that a number is algebraic or transcendental. Then it is usually meant that $k = \mathbb{Q}$.

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

Theorem 4.4. *If α is an algebraic element, then $k[\alpha] = k(\alpha) \cong k[x]/\langle p(x)\rangle$ is a finite extension of k. Conversely if $k[\alpha]$ is a finite extension of k, then α is algebraic.*

[1] This means that if $a_1x_1 + \cdots + a_nx_n = 0$, then $a_1 = a_2 = \cdots = a_n = 0$.
[2] This means that every $x \in V$ can be written in the form $a_1x_1 + \ldots a_nx_n$ for some $a_i \in k$.

Proof. Left to the reader, use previous exercises from this worksheet. For the second part, you can use an idea similar to the proof of Proposition 4.6. □

Definition 4.5. An extension of fields $k \subseteq K$ is called *algebraic* if every element of K is algebraic over k.

Proposition 4.6. *If $k \subseteq K$ is a finite extension of fields, then it is an algebraic extension. In particular, if α is algebraic over k, then $k[\alpha]$ is an algebraic extension.*

Proof. For the first statement, choose $\alpha \in K$. Then consider the set

$$B_n = \{1, \alpha^1, \alpha^2, \ldots, \alpha^n\}$$

For big enough n, B_n is linearly dependent because K is a finite dimensional k-vector space. Let n be the first integer such that B_n is linearly dependent over k. Then $\alpha^n = \lambda_0 1 + \lambda_1\alpha^1 + \lambda_2\alpha^2 + \cdots + \lambda_{n-1}\alpha^{n-1}$ for some $\lambda_i \in k$. But then we have constructed a polynomial of which α is a root, namely

$$x^n - \lambda_{n-1}x^{n-1} - \cdots - \lambda_1 x^1 - \lambda_0.$$

For the second statement, any $\beta \in k[\alpha]$ is algebraic since $k[\alpha]$ is a finite extension of k. □

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.

5. Splitting fields

Definition 5.1. Suppose that k is a field and $p(x) \in k[x]$ is any polynomial, irreducible or not. A *splitting field for $p(x)$ over k* is a field extension $k \subseteq K$ such that:

(1) $p(x)$ splits as an element of $K[x]$. In other words, if within $K[x]$, $p(x)$ factors into a product of linear factors.
(2) There is no subfield $L \subsetneq K$, such that both $k \subseteq L$ and $p(x)$ splits in L.

Theorem 5.2 (Existance and Uniqueness)**.** *Given any polynomial $p(x) \in k[x]$, there is always a splitting field $K \supseteq k$ for $p(x)$ over k. Furthermore, any two such splitting field are isomorphic.*

Proof. See Rotman, Proposition 5.16 and 5.22. □

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 $x^4 - 5$.

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