Roots and Irreducibility

All of the facts listed below are proved in any abstract algebra book, e.g. Dummit and Foote.

Assumptions. Suppose that F is a field.

Roots

Definition 1. Suppose that $f(\lambda) \in F[\lambda]$. A *root* of $f(\lambda)$ in F is an element $c \in F$ so that $f(c) = 0$.

Proposition 2 (The factor theorem). *Suppose that $f(\lambda) \in F[\lambda]$ and $c \in F$. Then,*

$$c \text{ is a root of } f(\lambda) \iff \lambda - c \mid f(\lambda).$$

To find the roots of a polynomial $f(\lambda)$ is a polynomial over $\mathbb{Q}$, one can first multiply the polynomial by the least common multiple of the denominators of the coefficients in order to get a polynomial over $\mathbb{Z}$ which has the same roots. To handle such polynomials, the following proposition is useful.

Proposition 3 (Finding roots in $\mathbb{Q}$). *Suppose that*

$$f(\lambda) = a_n\lambda^n + \cdots + a_1\lambda + a_0 \in \mathbb{Z}[\lambda],$$

where $n \geq 1$ and $a_n \neq 0$. Suppose that $c = \frac{r}{s} \in \mathbb{Q}$, where $r, s \in \mathbb{Z}$, $s > 0$ and $gcd(r, s) = 1$. If c is a root of $f(\lambda)$, then $r \mid a_0$ and $s \mid a_n$.

Example 4. Suppose that $f(\lambda) = 2\lambda^3 + \lambda + 1 \in \mathbb{Z}[\lambda]$. Suppose that $c = \frac{r}{s} \in \mathbb{Q}$, where $r, s \in \mathbb{Z}$, $s > 0$ and $gcd(r, s) = 1$. (Any rational number can be written in this form.) If c is a root of $f(\lambda)$, then by Proposition 3, we have $r \mid 1$ and $s \mid 2$. Thus, $r = \pm 1$ and $s = 1$ or 2. So $c = \pm 1$ or $\pm\frac{1}{2}$. However, none of these are roots of $f(\lambda)$. Hence, $f(\lambda)$ has no roots in $\mathbb{Q}$.

Irreducibility

Definition 5. Suppose that $f(\lambda)$ is a polynomial of degree $n \geq 1$ in $F[\lambda]$. We say that $f(\lambda)$ is *reducible* in $F[\lambda]$ if there exist polynomials $g(\lambda)$ and $h(\lambda)$ of smaller degree than n in $F[\lambda]$ so that

$$f(\lambda) = g(\lambda)h(\lambda).$$

Otherwise, we say that $f(\lambda)$ is *irreducible* over F.

Example 6. Any polynomial of degree 1 over F is irreducible over F. If $F = \mathbb{C}$, degree 1 polynomials are the only irreducible polynomials over F (by the Factor Theorem and the Fundamental Theorem of Algebra).

The following fact follows easily from the Factor Theorem:

Typeset by $\mathcal{AMS}$-TEX

Proposition 7. *Suppose that $f(\lambda)$ is a polynomial of degree 2 or 3 over F. Then,*

$$f(\lambda) \text{ is irreducible over } F \iff f(\lambda) \text{ has no roots in } F.$$

Example 8. Suppose that $f(\lambda) = 2\lambda^3 + \lambda + 1 \in \mathbb{Z}[\lambda]$. We saw in Example 4 that $f(\lambda)$ has no roots in $\mathbb{Q}$. Hence, since $f(\lambda)$ has degree 3, it follows from Proposition 7 that $f(\lambda)$ is irreducible over $\mathbb{Q}$.

To show that a polynomial $f(\lambda)$ over $\mathbb{Q}$ is irreducible, one can first multiply the polynomial by the least common multiple of the denominators of the coefficients in order to get a polynomial over $\mathbb{Z}$. (This does not change affect irreducibility.) To handle such polynomials, the following proposition is useful.

Proposition 9 (Eisenstein's criterion for polynomials over $\mathbb{Z}$). *Suppose that*

$$f(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} \cdots + a_1\lambda + a_0 \in \mathbb{Z}[\lambda],$$

where $n \geq 1$ and $a_n \neq 0$. Suppose that there exists a prime integer p so that

$$p \mid a_i \quad \text{for } 0 \leq i \leq n-1,$$
$$p \nmid a_n \quad \text{and} \quad p^2 \nmid a_0.$$

Then, $f(\lambda)$ is irreducible over $\mathbb{Q}$.

Example 10. Let $f(\lambda) = \lambda^{22} - 28\lambda + 50 \in \mathbb{Z}[\lambda]$. By Eisenstein's criterion with $p = 2$, $f(\lambda)$ is irreducible over $\mathbb{Q}$.

Example 11. Let

$$f(\lambda) = \lambda^{p-1} + \lambda^{p-2} + \cdots + \lambda + 1 \in \mathbb{Z}[\lambda],$$

where p is a positive prime. ($f(\lambda)$ is called the *cyclotomic* polynomial of degree p.) Let $g(\lambda) = f(\lambda + 1)$. One can show that $g(\lambda)$ satisfies the hypotheses of Eisenstein's criterion (using the fact that $f(\lambda) = \frac{\lambda^p - 1}{\lambda - 1}$ and hence $g(\lambda) = \frac{(\lambda+1)^p - 1}{\lambda}$). Thus, $g(\lambda)$ is irreducible over $\mathbb{Q}$, and so $f(\lambda)$ is irreducible over $\mathbb{Q}$.

The characteristic of a field

Suppose that F is a field.
If $n \in \mathbb{Z}$ and $a \in F$, we define

$$na = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ factors}} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ \underbrace{(-a) + \cdots + (-a)}_{-n \text{ factors}} & \text{if } n < 0. \end{cases}$$

Then,

$$\begin{gathered} (m+n)a = ma + na, \quad n(ma) = (nm)a, \\ n(a+b) = na + nb \quad \text{and} \quad n(ab) = (na)b = a(nb) \end{gathered} \tag{1}$$

for $m, n \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$.

It follows easily from (1) that the set $\{n \in \mathbb{Z} : n1 = 0\}$ is an ideal of $\mathbb{Z}$. Hence, since $\mathbb{Z}$ is a pid, there exists a unique integer $p \geq 0$ so that

$$\{n \in \mathbb{Z} : n1 = 0\} = (p). \tag{2}$$

p is called the *characteristic* of F, and we write $\text{char}(F) = p$.

There are two possibilites:

(i) $p = 0$. This means that the only integer n so that $n1 = 0$ is $n = 0$.

(ii) $p > 0$. This means that there exists a nonzero integer n so that $n1 = 0$. In that case p is the smallest integer ≥ 1 so that

$$p1 = 0$$

in F. It is easy to show (see problem #6(a) on this assignment) that p is a prime in this case.

Notes: Let $p = \text{char}(F)$.

(i) Suppose that $p = 0$. Then, if $n \in \mathbb{Z}$, we have by (2) that

$$n1 = 0 \iff n = 0.$$

Moreover, if $a \neq 0$ in F and $n \in \mathbb{Z}$, then $na = 0 \iff n(a1) = 0 \iff a(n1) = 0 \iff n1 = 0$ (since F is a field) $\iff n = 0$. Hence, if $a \neq 0$ in F and $n \in \mathbb{Z}$,

$$na = 0 \iff n = 0.$$

(ii) Suppose that $p > 0$. Then, if $n \in \mathbb{Z}$, we have by (2) that

$$n1 = 0 \iff p \mid n.$$

Moreover (arguing as in (i)) if $a \neq 0$ in F and $n \in \mathbb{Z}$,

$$na = 0 \iff p \mid n.$$