August 31:

Math 432 Class Lecture Notes

- Quotient rings
- Root fields
- Splitting fields

0.1 Quotient rings

Several questions have been raised, in class and in connection with the homework, that come down to how to interpret quotient rings. If R is a ring and I is an ideal then the quotient ring R/I is the of equivalence classes in R under the equivalence relation

$$x \sim y \quad \text{if and only if} \quad x - y \in I.$$

Often these equivalence classes are most easily understood by choosing convenient or natural "representatives" from each equivalence class.

Example 1. It is often convenient to think of $\mathbf{Z}/n\mathbf{Z}$ as the set

$$\{0, 1, \cdots, n-1\}$$

with addition and multiplication "modulo n" rather than a more unwieldy set of n infinite sets. If x is any integer then there is a unique integer r so that

$$x = qn + r, \quad 0 \leq r < n$$

and this shows that every integer is in the equivalence class of a unique r, $0 \leq r < n$.

Example 2. If f is a nonzero polynomial then $F[x]/(f)$ is a set of equivalence classes. The division algorithm

$$g = qf + r$$

shows that there is a unique element of each equivalence class whose degree is less than $n := \deg(f)$ and it is customary to think of the quotient as the set of all polynomials

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

of degree less than n with coefficients in F.

0.2 Root fields

If E is an extension of F and α is an element of E then last time we found a minimal polynomial $m_\alpha(x)$ that is monic, has α as a root, and is a divisor of any polynomial that has α as a root. The polynomial m_α is irreducible and

$$F(\alpha) \simeq F[x]/m_\alpha.$$

Finally, the powers of α, α^k, $0 \leq k < n$ form a basis for the extension $F(\alpha)/F$.

Now suppose that we start with an irreducible polynomial $f(x)$ and we want to construct an extension field in which f has a root. This is easy! Namely, the irreducibility of f implies that the quotient ring

$$F[x]/(f)$$

is actually a field, and the equivalence class containing x is a root of f, tautologically.

Definition 3. If $f \in F[x]$ is irreducible then a **root field** for f is a field E containing a root α of f such that $E = F(\alpha)$.

Theorem 4. Root fields exist, and they are unique, i.e. if E and E' are root fields with roots α and α', respectively, then there exists an isomorphism $\phi : E \to E'$ such that $\phi(\alpha) = \alpha'$, and $\phi(x) = x$ for all $x \in F$.

Indeed, suppose that E is a root field. Map $F[x]$ to E by evaluating polynomials at α. Since $E = F(\alpha)$ we see that

$$F[x]/(f) \simeq F(\alpha) = E.$$

Since any root field is isomorphic to $F[x]/(f)$ it follows that any two root fields are isomorphic, and from the proof we see that there is an isomorphism with the stated property.

Example 5. There are three root fields of $f(x) = x^3 - 2$ inside the complex numbers. Namely, let

$$f(x) = x^3 - 2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

where $\alpha_1 = \sqrt[3]{2}$ is the real cube root of 2, $\alpha_2 = \omega\alpha_1$, $\alpha_3 = \omega^2\alpha_1$, where $\omega = (-1 + \sqrt{3}i)/2 = \exp(2\pi i/3)$ is a third root of unity. The field $\mathbf{Q}(\alpha_1)$ is a subfield of the real numbers and is therefore not equal to either $\mathbf{Q}(\alpha_2)$ or $\mathbf{Q}(\alpha_3)$, neither of which are contained in the real numbers.

This leaves open the possibility that $\mathbf{Q}(\alpha_2)$ and $\mathbf{Q}(\alpha_3)$ are the same field. Any field containing both α_2 and α_3 would contain their quotient $\omega = \alpha_3/\alpha_2$. However, the minimal polynomial of ω is easily checked to be $m_\omega(x) = x^2 + x + 1$, so $\mathbf{Q}(\omega)$ is of degree 2 over $\mathbf{Q}$. The equation

$$3 = [\mathbf{Q}(\alpha_2) : \mathbf{Q}] = [\mathbf{Q}(\omega) : \mathbf{Q}][\mathbf{Q}(\alpha_2) : \mathbf{Q}(\omega)]$$

is nonsensical, and this contradiction shows that $\mathbf{Q}(\alpha_2)$ and $\mathbf{Q}(\alpha_3)$ are distinct.

0.3 Splitting fields

Definition 6. If $f(x)$ is any nonzero polynomial in $F[x]$, then an extension E of F is said to be a splitting field of f over F if $f(x)$ factors into linear factors in $E[x]$, and no proper subfield of E has this property.

Theorem 7. Splitting fields exist and are unique, up to isomorphism.

We'll prove existence by induction on the degree, and leave uniqueness (and some cool applications) until next time.

Let $n = \deg(f)$ be the degree of a polynomial $f(x) \in F[x]$. The case $n = 1$ of the existence part of the theorem is trivial.

Now suppose that all polynomials over any field with degree less then n have splitting fields. Choose $g(x) \in f[x]$, of positive degree, that divides f and is irreducible over F. Let E be the root field of g, and let α be a root of g in E.

Now, over E, f has at least one linear factor, namely $f(x) = (x - \alpha) f_1(x)$ for some $f_1 \in E[x]$. Now $\deg(f_1) < n$ so by the induction hypothesis, there exists a splitting field of f_1, call it E'. Since f_1 splits in $E'[x]$ it follows that f splits into linear factors in E'. The smallest field containing the roots of f is a splitting field. (In fact, as checked in class, E' is the smallest field containing the roots.)