Wikipedia assignment: history of some algebra problems?

5.3. Introduction fo Field Extensions

Earlier : Showed that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field.
We can think of this as a vector space with coefficients in $\mathbb{Q}$ and basis $\{1, \sqrt{2}\}$.
Recall also that it is isomorphic to $\mathbb{Q}[x]/(x^2 - 2)$.
In fact any field extension of a field F with a finite basis (hence finite dimension) can be generated in this way.
Proof: Basically "rationalizing the denominator."
But another way to prove: example $1 + \sqrt{2} = u$ has inverse $u - 2$. This can be generalized:
Also, note that there can be no extension between $\mathbb{Q}$ and $K = \mathbb{Q}[\sqrt{2}]$.
Reason: Use Problem 17: V a vector space over K and K an extension over F then $dim_F V = dim_K V \times dim_F K$. Here $F = \mathbb{Q}$.

Definition $\alpha \in K$ is *algebraic over* $F \subset K$ if it is the root of a polynomial in $F[x]$.
Also, the field K is an algebraic extension of F if all elements in K are algebraic over F.

Minimal polynomial
If $\alpha \in K$ is *algebraic over* $F \subset K$ there is a minimal polynomial $p(x)$ that is monic, with $p(\alpha) = 0$.
Morevoer the minimal polynomial is also irreducible.
Hence $(p(x)) = M$ is a maximal ideal (because $F[x]$ is a PID!) and $F[x]/M$ is a field.

If $\alpha \in K$ is algebraic over F then $F[\alpha]$ is a finite dimensional field over F.
Every $\beta \in F[\alpha]$ is also algebraic over F.
In fact any finite dimensional extension is an algebraic extension.

Key points to be used:

1. *Any set with more than n vectors will be linearly dependent*
2. *$F[\alpha]$ is a vector space of dimension equal to degree of minimal polynomial.*
3. *$F[\alpha]$ is a field.*
4. *$F[\alpha] \simeq F[x]/M$.*

More generally, if D is an integral domain with 1 then
if D is a finite dimensional vector space over F then D is a field.
Here $D = F[\alpha]$.

Problem: Describe $\mathbb{Z}[\mathbf{x}]/(\mathbf{x} + \mathbf{1})$
What do the cosets look like?
Can two integers be in the same coset of $(x + 1)$?
If $m + (x + 1) = n + (x + 1)$ then $n - m \in (x + 1)$, which is impossible.
So $n + (x + 1) \in \mathbb{Z}[x]/(x + 1)$ are distinct cosets, for $n \in \mathbb{Z}$.
What about $f(x) + (x + 1)$ where $f(x) \in \mathbb{Z}[x]$?
Using Euclidean algorithm, $f(x) + (x + 1) = n + (x + 1)$
where n is the remainder upon dividing $f(x)$ by $x + 1$.
Note that $\mathbb{Z}[x]$ is not Euclidean, but you can divide any polynomial by $x + 1$ by just writing the remainder as $f(-1)$.
So $\mathbb{Z}[x]/(x + 1) \simeq \mathbb{Z}$.
$\mathbb{Z}[x]$ is not Euclidean because when you divide one integer polynomial by another you don't always get an integer as the quotient or the remainder.
In the case of $x + 1$ both are in $\mathbb{Z}[x]$ because you can write $f(x) = f((x + 1) - 1)$, then expand it and collect terms with $x + 1$ to write it as $q(x)(x + 1) + n$ where $q(x) \in \mathbb{Z}[x]$.

Problem 11: Transcendental extension generated by a transcendental element a is simply $F(a)$.

Note: If a is transcendental, then so is $f(a)$ for any $f \in F[x]$. This is basically problem 8 in 5.3.

Problem 12: Transcendental extension $F(a)$ is isomorphic to $F(x)$, the field of rational functions in x over F.

Problem 15: Example of $F \subset K$ such that K is algebraic but not finite extension of F.

Basically, transcendental extensions are infinite and finite extensions are algbraic, but algebraic extensions need not be all finite

Answer: Let $F = \mathbb{Q}$ and $K = \cup F[\{u_{q_1}, u_{q_2}, ..., u_{q_n}\}]$ where u_{q_i} is a root of $x^q - p$ for a fixed prime p, and the $q_i's$ are all the primes $\neq p$ in ascending order 2,3,5,7,....

$x^n - p$ is irreducible (Eisenstein's criterion) and monic, hence it is the minimal polynomial of u_{q_i}, so $F[u_{q_i}] \subset K$ is an algebraic extension of degree q.

Any $\alpha \in K$ is algebraic because it has to belong to $F[\{u_{q_1}, u_{q_2}, ..., u_{q_n}\}]$ for some n.

Each of these extensions being finite, all their elements are algebraic.

On the other hand the union K is infinite because any finite extension would have to have a finite dimension n and n can be divisible by only a finite number of primes.

The degree of $F[\{u_{q_1}, u_{q_2}, ..., u_{q_n}\}]$ for instance, would be divisible by all the primes $q_1, q_2, ..., q_n$.

HW8:

5.2: 1,6,8,10,11,14. 5.3: 1,2,3,5,7,8,9,13,14