MATH 532
EXERCISES 1

A. ZEYTİN

Unless otherwise stated K and k are fields and K/k is a field extesion.

(1) Show that a subring K' of K is a subfield whenever K' is closed under multiplication.

(2) Perform the following polynomial divisions (i.e. find q and r so that $f = gq+r$ within the indicated polynomial rings):
- ▶ $f(X) = X^2 + 7X + 12$, $g(X) = X + 3$ in $\mathbf{Q}[X]$,
- ▶ $f(X) = X^2 + 7X + 12$, $g(X) = X + 3$ in $(\mathbf{Z}/17\mathbf{Z})[X]$,
- ▶ $f(X) = X^2 + 7X + 12$, $g(X) = X + 3$ in $(\mathbf{Z}/7\mathbf{Z})[X]$,
- ▶ $f(X) = X^3 + 4X + 6$, $g(X) = X^2 + 1$ in $\mathbf{Q}[X]$,
- ▶ $f(X) = X^3 + 4X + 6$, $g(X) = X^2 + 1$ in $(\mathbf{Z}/7\mathbf{Z})[X]$,
- ▶ $f(X) = X^3 + 4X + 6$, $g(X) = X^2 + 1$ in $(\mathbf{Z}/3\mathbf{Z})[X]$,

(3) Find the greatest common divisor of the following polynomials:
- ▶ $f(X) = 3X^3 + 4X^2 + 3$, $g(X) = 3X^3 + 4X^2 + 3X + 4$ in $(\mathbf{Z}/5\mathbf{Z})[X]$,
- ▶ $f(X) = X^2 + 7X + 6$, $g(X) = X^2 - 5X - 6$ in $\mathbf{Q}[X]$,

(4)
- ▶ Recall the definition of a Euclidean domain, R.
- ▶ Let R be a Euclidean domain with Euclidean norm N and I be an ideal of R. Show that for any $f \in I$ with smallest norm in I we have $I = (f)$.

(5) Show that if $f(X) \in K(X)$ is a polynomial of degree 2 or 3, then f is irreducible if and only if f has a root in K. Show by an example that this may not be true if the degree of f is greater than or equal to 4.

(6) Decide whether the following polynomials are irreducible over the indicated fields:
- ▶ $f(X) = X^2 + 1$ over $K = (\mathbf{Z}/2\mathbf{Z})[X]$
- ▶ $f(X) = X^2 + 1$ over $K = (\mathbf{Z}/3\mathbf{Z})[X]$
- ▶ $f(X) = X^3 + X + 1$ over $K = (\mathbf{Z}/2\mathbf{Z})[X]$
- ▶ $f(X) = X^3 + X + 1$ over $K = (\mathbf{Z}/3\mathbf{Z})[X]$
- ▶ $f(X) = X^4 + 12X^2 + 6$ over $K = \mathbf{Q}[X]$

(7) The software I have advertised in class (PARI/gp) can handle polynomial division modulo distinc fields. It is available at

```
https://pari.math.u-bordeaux.fr
```

Its syntax is pretty simple : e.g. type

```
factor(X^2 +3*X - 4)
```

to see that the polynomial $f(X) = X^2 + 3X - 4$ is reducible. To find factorization of f in $\mathbf{Z}/7\mathbf{Z}$ just type :

```
factormod(X^2 +3*X - 4,7)
```

Try the software and look for fields over which f is reducible and irreducible. Repeat the same exercise with the polynomial $g(X) = X^4 - 10X^2 + 1$ and make some observations on its irreducibility.

(8) Let p be any prime number and set $f_p(X) = 1 + X + X^2 + \ldots + X^{p-1}$.
- ▶ Show that for any polynomial $f(X) \in K[X]$, $f(X+1)$ is irreducible if and only if $f(X)$ is irreducible.
- ▶ Use previous part to show that $f_p(X)$ is irreducible.

(9) Repeat the previous exercise for the polynomial $f(X) = X^4 + 4X^3 + 6X^2 + 2X + 1$ by replacing $X+1$ with $X-1$.

(10) Let $f(X) \in K(X)$ be a monic polynomial in $K[X]$. Let

$$f(X) = (f_1(X))^{n_1} (f_2(X))^{n_2} \cdots (f_l(X))^{n_l}$$

be the factorization of f into irreducible factors; where $n_i \in \mathbf{N}$. Show that the rings $K[X]/(f(X))$ and

$$K[X]/\left((f_1(X))^{n_1}\right) \times K[X]/\left((f_2(X))^{n_2}\right) \times \cdots \times K[X]/\left((f_l(X))^{n_l}\right)$$

are isomorphic. This is the so-called generalized chinese remainder theorem.

(11) Express propositons 3, 4 and 5 of our notes using UFD's instead of $\mathbf{Z}$, their fields of fractions instead of $\mathbf{Q}$ and prime ideals instead of prime numbers.

(12) Show that if R and S are two subrings of a field K then their intersection is again a subring. In particular $k[S]$ is the intersection of all rings containing k and S.

(13) Show that if R and S are two subfields of a field K then their intersection is again a field. In particular $k(S)$ is the intersection of all fields containing k and S.

(14) Give the construction of a field with 8 and 9 elements. Write the multiplication tables.

(15) Let K/k and L/K be two extensions. (We usually write $L/K/k$ in such a case and call it a tower.) Show that L/k is an algebraic extension if and only if L/K and K/k are algebraic extensions.

(16) Find the minimal polynomials of the following elements over the indicated fields and hence deduce that they are algebraic over the indicated fields
- $\sqrt[6]{2}$ over $\mathbf{Q}$,
- $\sqrt[6]{2}$ over $\mathbf{Q}(\sqrt{2})$,
- $\sqrt[6]{2}$ over $\mathbf{Q}(\sqrt[3]{2})$,
- $\sqrt[3]{x}$ over $\mathbf{Q}(x)$,