Aakash Ghosh
Email: ag19ms129@iiserkol.ac.in
Course: Algebra III

ID: 19MS129
Term: Autumn 2022

1 Problem Sheet 1

Problem 1.5

Let $F \hookrightarrow K$ be a field extension and $a, b \in K$ be algebraic over F with minimum polynomials of degree p, q, where p, q are distinct prime numbers. Show that $[F(a,b) : F] = pq$.

Solution: Note that as $[F(a) : F] \mid [F(a,b) : F]$ and $[F(b) : F] \mid [F(a,b) : F]$, $[F(a,b) : F]$ is of the form kpq. Let $\{\alpha_i\}_{1\leq i\leq p}$ be a basis of $F(a) \mid_F$ and $\{\beta_j\}_{1\leq j\leq q}$ be a basis of $F(b) \mid_F$. Consider the field F' spanned by $\{\alpha_i\beta_j\}_{1\leq i\leq p, 1\leq j\leq q}$. $a, b \in F'$ and therefore $F(a,b) \subseteq F'$. By our construction $[F' : F] \leq pq$. Therefore, $[F(a,b) : F] \leq pq$. It follows that $k = 1$ which completes the proof.

Problem 1.1

Determine

1. $[\mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}]$
2. $[\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7}), \mathbb{Q}]$
3. $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}), \mathbb{Q}]$

Solution: We shall use the result of problem 1.5 proved above.

Lemma 1. *If p is prime, then $x^n - p$ is irreducible over $\mathbb{Q}$ for $n > 1$.*

Proof. By applying Einstein's criteria over p on $x^n - p$ we get $x^n - p$ is irreducible over $\mathbb{Z}$. By Gauss lemma, we conclude that $x^n - p$ is irreducible over $\mathbb{Q}$ too. □

1. Note that $\sqrt{2}$ satisfies $x^2 - 2 = 0$. By lemma 1, this polynomial is irreducible and therefore $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Note that $x^2 - 5 = 0$ has $\sqrt{5}$ as root. Therefore, the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{2})$, $p(x)$, divides $(x^2 - 5)$. We show p is not linear, i.e. $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$. Assume to the contrary and let $\sqrt{5} = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Then we note:
$$\begin{aligned}\sqrt{5} &= a + b\sqrt{2}\\ \Rightarrow 5 &= a^2 + 2b^2 + 2ab\sqrt{2}\\ \Rightarrow \sqrt{2} &= \frac{5 - a^2 - 2b^2}{2ab} \in \mathbb{Q}\end{aligned}$$
Which is a contradiction. Therefore, $p(x)$ has degree 2. It follows that
$$[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$
2. Like before, note that $x^2 - 7 = 0$ has $\sqrt{7}$ as root. Therefore, the minimal polynomial of $\sqrt{7}$ over $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, $p(x)$, divides $(x^2 - 7)$. Note that $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ and $\{1, \sqrt{5}\}$ is a basis of $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$. Therefore, as we pointed in Problem 1.5, $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ is a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ over $\mathbb{Q}$. We shall show $\sqrt{7} \notin \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Assume to the contrary and let $\sqrt{7} = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}$. Then:
$$\begin{aligned}\sqrt{7} &= a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}\\ \Rightarrow 7 &= (a^2 + 2b^2 + 5c^2 + 10d^2) + 2ab\sqrt{2} + \left(2ac + 2(bc + ad)\sqrt{2}\right)\sqrt{5}\\ \Rightarrow \sqrt{5} &= \frac{7 - \left((a^2 + 2b^2 + 5c^2 + 10d^2) + 2ab\sqrt{2}\right)}{2ac + (2bc + ad)\sqrt{2}} \in \mathbb{Q}(\sqrt{2})\end{aligned}$$

Which is a contradiction. Therefore, degree of p is two and

$$[\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7}):\mathbb{Q}(\sqrt{2},\sqrt{5})] \times [\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}] = 8$$

3. By Lemma 1, x^2-3 and x^3-2 are irreducible. As $\sqrt{3}, \sqrt[3]{2}$ are roots of those polynomials, $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2, [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$. By Problem 1.5, it follows that $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}),\mathbb{Q}] = 2 \times 3 = 6$

Problem 1.2

Prove that finite fields can't be algebraically closed.

Solution: Let $\mathbb{F}$ be a finite field. Consider the polynomial $p(x) = \prod_{\alpha\in\mathbb{F}}(x-\alpha)+1$. This polynomial has no roots in $\mathbb{F}$. Consider the splitting field $\mathbb{F}'$ of p over $\mathbb{F}$. Therefore, there exists a proper algebraic extension of $\mathbb{F}$ and $\mathbb{F}$ is not closed.

Problem 1.3

Prove that any extension of prime order (i.e., the degree is prime) is simple.

Solution: Let K be a prime order extension of F. Let $\alpha \in K$ such that $\alpha \notin F$. Since $[F(\alpha):F] \mid [K:F(\alpha)] = p$, it follows that $[F(\alpha):F]$ is either 1 or p. But as $\alpha \notin F$ it follows that $[F(\alpha):F] = p$. Therefore, $[K:F(\alpha)] = \frac{[K:F]}{[F(\alpha):F]} = 1$. Therefore, $K = F(\alpha)$ and K is simple.

Problem 1.4

Is $\mathbb{Q}(\sqrt{2},\sqrt{5})$ simple?

Solution: Yes. We show $\mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(\sqrt{2}+\sqrt{5})$. It is easy to see that $\mathbb{Q}(\sqrt{2}+\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{5})$ as $\sqrt{2}+\sqrt{5} \in \mathbb{Q}(\sqrt{2},\sqrt{5})$. Let $p(x)$ be the minimal polynomial of $\sqrt{2}+\sqrt{5}$ over $\mathbb{Q}$. Now as $\sqrt{2}+\sqrt{5}$ is irrational, p is not linear. Assume p is quadratic and there exists rational b, c such that x^2+bx+c has $\sqrt{2}+\sqrt{5}$ as roots. Then on putting $x = \sqrt{2}+\sqrt{5}$ we get:

$$\begin{aligned}
&(\sqrt{2}+\sqrt{5})^2 + b(\sqrt{2}+\sqrt{5}) + c = 0\\
\Rightarrow &7 + c + b\sqrt{2} + (b+2\sqrt{2})\sqrt{5} = 0\\
\Rightarrow &\sqrt{5} = -\frac{7+c+b\sqrt{2}}{b+2\sqrt{2}} \in \mathbb{Q}\sqrt{2}
\end{aligned}$$

Which is not possible as shown in problem 1.1(part 1). Therefore, p is not quadratic. Now we have $deg(p) = [\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q}] > 2$. By problem 1.1 we have $[\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}] = 4$. As $[\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}]$, the only possible value of $[\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q}]$ is 4. It follows that $[\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{5})] = [\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}]/[\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q}] = 1$. Therefore, $\mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(\sqrt{2}+\sqrt{5})$ and $\mathbb{Q}(\sqrt{2},\sqrt{5})$ is simple.

Problem 1.6

Show that an extension $F \hookrightarrow K$is algebraic if and only if every ring R with $F \subseteq R \subseteq K$ is a field.

Solution: Let K be algebraic. We show that R is a field. To show this we only need to show that if $\alpha \in R$, $\alpha^{-1} \in R$. As K is algebraic, there exists some polynomial $p(x)$ such that $p(\alpha) = 0$. Let

$p = \sum_{i=0}^{n} a_i x^i$ where $a_i \in F$. We assume p is irreducible and therefore $a_0 \neq 0$. Then

$$\begin{aligned}
&\sum_{i=0}^{n} a_i \alpha^i = 0 \\
\Rightarrow &\sum_{i=1}^{n} a_i \alpha^i = -a_0 \\
\Rightarrow &\alpha \left(\sum_{i=1}^{n} a_i \alpha^{i-1} \right) = -a_0 \\
\Rightarrow &\alpha \left[\frac{1}{-a_0} \left(\sum_{i=1}^{n} a_i \alpha^{i-1} \right) \right] = 1
\end{aligned}$$

Therefore, α has an inverse and R is a field.

Now we assume all such K are fields. We show F is algebraic. We prove by contradiction. Assume there exists a transcendental element α. Then $F[\alpha] \equiv F[X]$. Consider the ring $F[X]$. We show that this is not a field. Let $p(x)$ be a non-zero polynomial with an inverse $q(x)$ over K. Then: $p(\alpha)q(\alpha) = 1 \Rightarrow p(\alpha)q(\alpha) - 1 = 0$. Therefore, $pq - 1$ has α as a root which contradict the fact that α is transcendental. Therefore, no such α exist and F is algebraic.

Problem 1.7

Let $F \hookrightarrow K$ be a field extension and $a \in K$ with its minimal polynomial of degree m. Show that $m \mid [K : F]$.

Solution: We note that $m = [F(a) : F]$ and by tower lemma: $[K : F] = [K : F(a)][F(a) : F]$. The solution follows.

Problem 1.8

Does there exist a polynomial $f(X) \in \mathbb{Z}[X]$ of degree at least 2 such that $f(X)$ is irreducible over $\mathbb{Z}_p[X]$ for each prime p?

Solution: No. Without loss of generality assume leading term of f is positive and GCD of all coefficients of $f = 1$. Then $\lim_{x\to\infty} f(x) = \infty$. Therefore, there exist some natural n such that $f(n) = \alpha > 1$. Let p(which can be α itself) be a prime factor of α. Let denote $[x]$ to be the equivalence class of x such that $x \equiv [x] (\mod p)$. If $f(x) = \sum_{i=1}^{r} c_i x^i$, then note that:

$$[f]\left([n]\right) = \sum_{i=1}^{r} [c_i]\,[n]^i = \left[\sum_{i=1}^{r} c_i n^i\right] = [\alpha] = 0$$

Therefore, f has a root in $\mathbb{Z}/p\mathbb{Z}$ and is reducible.

Problem 1.9

Let $\overline{\mathbb{Q}} := \{x \in \mathbb{C} \mid x \text{ is algebraic over } \mathbb{Q}\}$. Is $[\overline{\mathbb{Q}} \mid \mathbb{Q}]$ finite?

Solution: Let p be a prime. Consider the equation $f_p(x) = x^p + p$. Let α_p be the root. It follows minimal polynomial of α_p divides f_p. But f_p is irreducible by Einstein's criteria and Gauss's lemma. Therefore, minimal polynomial of α_p is f_p and $[\mathbb{Q}(\alpha_p) : \mathbb{Q}] = p$. As α_p is algebraic, $\alpha_p \in \overline{\mathbb{Q}}$. Therefore, $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha_p) \hookrightarrow \overline{\mathbb{Q}}$ and $p \mid [\overline{\mathbb{Q}} : \mathbb{Q}]$. As this is true for all primes p and as there are infinite primes, $[\overline{\mathbb{Q}} : \mathbb{Q}]$ is not finite.

Problem 1.10

Prove that there exists a field F such that
(a) F is infinite,
(b) F is algebraic over a finite field, and
(c) F is not algebraically closed

Solution:

2 Problem sheet 2

Problem 2.1

Find the degree of the splitting fields.

1. $f(X) = X^4 - 2 \in \mathbb{Q}(X)$ over $\mathbb{Q}$
2. $f(X) = X^4 + 1 \in \mathbb{Q}(X)$ over $\mathbb{Q}$

Solution:

1. The roots of f are $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. The splitting field contains $\sqrt[4]{2}$ and i. The smallest such field is $\mathbb{Q}(\sqrt[4]{2}, i)$. By applying Einstein's criteria on f we conclude f is irreducible. As $\sqrt[4]{2}$ is a root of f, we conclude f is minimal polynomial of $\sqrt[4]{2}$ and $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Now as i satisfies $p(x) = x^2 + 1$ and $i \notin \mathbb{Q}(\sqrt[4]{2})$, we conclude p is minimal polynomial of i over $\mathbb{Q}(\sqrt[4]{2})$. Therefore:
$$\text{order of splitting field} = [\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8$$
2. Let the splitting field be F. The roots of f are $\pm\frac{1}{\sqrt{2}} \pm i\frac{1}{\sqrt{2}}$. By adding the roots pairwise we get $\sqrt{2}, i \in F$. The smallest such field is $\mathbb{Q}[\sqrt{2}, i]$. It is shown before that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. As i satisfies $p(x) = x^2 + 1$ and $i \notin \mathbb{Q}(\sqrt{2})$, we conclude p is minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$. So we have $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$ Therefore:
$$\text{order of splitting field} = [\mathbb{Q}(\sqrt{2}, i), \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i), \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

Problem 2.2

Let $K \mid F$ be an extension of degree 2. Show that $K \mid F$ is normal.

Solution: Let for $\alpha \in K$, p be the minimal polynomial of α over F. Then p has degree 1 or 2. If p has degree 1 then p has a single root which is α, and we are done. Else let $p(x) = x^2 - bx + c = (x - \alpha)(x - \beta)$, where β is the other root of p. We need to show $\beta \in K$. Direct expansion shows that $b = \alpha + \beta \Rightarrow \beta = b - \alpha$. As K is a field, $\beta \in K$ which completes the proof.

Problem 2.3

Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3})|\mathbb{Q}$ is a normal extension.

Solution:

Lemma 2. $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

Proof. Assume to the contrary and let $\sqrt{3} = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Then we note:
$$\begin{aligned} &\sqrt{3} = a + b\sqrt{2} \\ \Rightarrow &3 = a^2 + 2b^2 + 2ab\sqrt{2} \\ \Rightarrow &\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q} \end{aligned}$$
Which is a contradiction. $\square$

Lemma 3. $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}=4]$

Proof. As shown in problem 1.1, $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. Note that $x^2-3=0$ has $\sqrt{3}$ as root. Therefore, the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$, $p(x)$, divides (x^2-3). We have shown p is not linear, i.e. $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$. Therefore, $p(x)$ has degree 2. It follows that

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\times[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=4$$

□

Lemma 4. $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Proof. It is easy to see that $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$ as $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$. Let $p(x)$ be the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$. Now as $\sqrt{2}+\sqrt{3}$ is irrational, p is not linear. Assume p is quadratic and there exists rational b,c such that x^2+bx+c has $\sqrt{2}+\sqrt{3}$ as roots. Then on putting $x=\sqrt{2}+\sqrt{3}$ we get:

$$\begin{aligned}&(\sqrt{2}+\sqrt{3})^2+b(\sqrt{2}+\sqrt{3})+c=0\\ \Rightarrow&5+c+b\sqrt{2}+(b+2\sqrt{2})\sqrt{3}=0\\ \Rightarrow&\sqrt{3}=-\frac{5+c+b\sqrt{2}}{b+2\sqrt{2}}\in\mathbb{Q}\sqrt{2}\end{aligned}$$

Which is not possible as shown in above. Therefore, p is not quadratic. Now we have $deg(p)=[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]>2$. We have shown $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$. As $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]\mid[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$, the only possible value of $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$ is 4. It follows that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{2},\sqrt{3})]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]/[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=1$. Therefore, $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$ □

Lemma 5. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *is the splitting field of* $(x^2-2)(x^2-3)$

Proof. Note that $f(x)=(x^2-2)(x^2-3)=(x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{3})(x-\sqrt{3})$. It is easy to see that the splitting field of f contains $\sqrt{2},\sqrt{3}$ and the smallest such field is $\mathbb{Q}(\sqrt{2},\sqrt{3})$. □

As $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field of f over $\mathbb{Q}$, it is a normal extension of $\mathbb{Q}$.

Problem 2.4

Prove that the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic

Solution: Assume $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are isomorphic and the isomorphism is given by ϕ. Then $\phi(1)=1$ and for any rational $r\in\mathbb{Q}$, $\phi(r)=r\phi(1)=r$. Let $p(x)=\sum_{i=1}^n c_ix^i$ be the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. Then note that:

$$\phi(p(x))=\phi\left(\sum_{i=1}^n c_ix^i\right)=\sum_{i=1}^n\phi(c_i)\phi(x)^i=\sum_{i=1}^n c_i\phi(x)^i=p\left(\phi(x)\right)$$

Putting $x=\sqrt{2}$ we conclude that $\phi\left(\sqrt{2}\right)$ is also a solution of $p(x)$. We have shown in problem 1.1 that $p(x)=x^2-2=(x-\sqrt{2})(x+\sqrt{2})$. Therefore, $\phi(\sqrt{2})\in\{\sqrt{2},-\sqrt{2}\}$. Assume $\sqrt{2}\in\mathbb{Q}(\sqrt{3})$ and let $\sqrt{2}=a+b\sqrt{3}$ where $a,b\in\mathbb{Q}$. Then we note:

$$\begin{aligned}&\sqrt{2}=a+b\sqrt{3}\\ \Rightarrow&2=a^2+3b^2+2ab\sqrt{3}\\ \Rightarrow&\sqrt{3}=\frac{3-a^2-3b^2}{2ab}\in\mathbb{Q}\end{aligned}$$

Which is a contradiction. It follows that $\pm\sqrt{2}\notin\mathbb{Q}(\sqrt{3})$. Which contradicts the fact that $\phi(\sqrt{2})\in\mathbb{Q}(\sqrt{3})$. Therefore, no such ϕ exists.

Problem 2.5

Let $f(X) := X^3 + X^2 + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$ and α be a root of f. Show that $\mathbb{Z}/2\mathbb{Z}(\alpha)$ is the splitting field.

Solution: Note that

$$0 = f(\alpha)^2 = (\alpha^3 + \alpha^2 + 1)^2 = \alpha^6 + \alpha^4 + 1 + 2(\alpha^5 + \alpha^3 + \alpha^2) = \alpha^6 + \alpha^4 + 1 = f(\alpha^2)$$

Therefore α^2 is also a root(Note: We can easily check that 1,0 are not roots of the equation. Therefore, $\alpha \neq \alpha^2$). By using Vieta's formula, we get -1 is the product of the roots and thus $-1/\alpha^3$ is also a root. As the splitting field contains α and the smallest field containing α also contains all the other roots, we conclude that $\mathbb{Z}/2\mathbb{Z}(\alpha)$ is the splitting field.

Problem 2.6

Let p be a prime. Show that the splitting field of $X^p - 1 \in \mathbb{Q}[X]$ is of degree $p-1$ over $\mathbb{Q}$.

Solution: Note if ζ is the p^{th} root of unity, then all the roots are given by ζ^r where $0 \leq r \leq p-1$. As the splitting field contains ζ and the smallest field containing ζ also contains all the other roots, we conclude that $\mathbb{Q}(\zeta)$ is the splitting field. Note that $X^p - 1 = (X-1)\left(\sum_{i=1}^{p-1} X^i\right)$. But As $\zeta \neq 1$, $\left(\sum_{i=1}^{p-1} \zeta^i\right) = 0$. We show $f(x) = \sum_{i=1}^{p-1} x^i$ is irreducible. Note that if $f(x)$ is irreducible if and only if $\tilde{f}(x) = f(x+1)$ is irreducible too (for if $f = hg$ then $\tilde{f} = h(x+1)g(x+1)$). Note that:

$$\tilde{f}(x) = f(x+1) = \frac{(x+1)^p - 1}{(x+1-1)} = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-1} \dots \binom{p}{i} x^{i-1} \dots + \frac{p(p-1)}{2}x + p$$

We can apply Einstein's criteria on $\tilde{f}$ to conclude it is irreducible. Therefore f is irreducible and is the minimal polynomial of ζ. It follows that order of splitting field= degree of $f = p-1$.

Problem 2.7

Suppose $K|F$ and $L|K$ are normal extensions. Is $L|F$ normal?

Solution: Let $F = \mathbb{Q}, K = \mathbb{Q}(\sqrt{2}), L = \mathbb{Q}(\sqrt[4]{2})$. Then $[K:F], [L:K] = 2$ and as shown in 2.2, they are normal extension. Consider the polynomial $p(x) = x^4 - 2$. We note p is irreducible over $\mathbb{Q}$ by Einstein's criteria. Assume $L|F$ is normal. As $\sqrt[4]{2}$ is a root of p then all roots of p lies in L. Note $i\sqrt[4]{2}$ is a root of p but is not in L, which is a contradiction. Therefore, $L|F$ is not normal and the statement is false.

Problem 2.8

Let $K_i|F$ be finite extensions for $1 \leq i \leq n$. Then there exists a finite normal extension $K|F$ and embeddings $\phi_i : K_i \xrightarrow{\sim} K$ such that $\phi_i|F = Id_F$.

Solution: Let K_i as each K_i is a finite extension, they are algebraic and are generated by adjoining a finite number of elements to F(one way to do so this is to adjoin elements one by one on F till no elements remain. As K_i has a finite order, this process stops in a finite number of steps). Let $K_i = F[\alpha_{(1,i)}, \alpha_{(2,i)} \dots]$. Consider the minimal polynomial $p_i = \prod_{i,j} p_{i,j}$ such that $p_{i,j}$ is the minimal polynomial of $\alpha_{i,j}$. Let K be the splitting field of p over F. As each $\alpha_{i,j} \in F$, F satisfies all the conditions mentioned above.

Problem 2.9

Let p be a prime integer and $n \geq 1$. What is the splitting field of $x^{p^n} - 1 \in \mathbb{Z}/p\mathbb{Z}$?

Solution: We note that in $\mathbb{Z}/p\mathbb{Z}$ we have:

$$x^{p^n} - 1 = x^{p^n} - 1 + \sum_{i=1}^{p-1} \binom{p}{i} \left(x^{p^{n-1}}\right)^i (-1)^{p-i} = (x^{p^{n-1}} - 1)^p$$

But in the same way we can write $(x^{p^{n-1}}-1)=(x^{p^{n-2}}-1)^p$ and so on. Continuing, we get $(x^{p^n}-1)=(x-1)^{p^n}$ in $\mathbb{Z}/p\mathbb{Z}$. Therefore, the only root is 1, and the splitting field is $\mathbb{Z}/p\mathbb{Z}$.

Problem 2.10

Let $K|F$ be a finite normal extension and $f(x)\in F[x]$ be irreducible. Let $g,h\in K[x]$ be two irreducible factors of f in $K[x]$. Show that there exists an F-isomorphism $\sigma : K \xrightarrow{\sim} K$ that takes g to h

3 Problem sheet 3

Problem 3.1

Check whether $X^4+X+1\in\mathbb{Q}[X]$ is a separable polynomial.

Solution: $Df=4X^3+1$. Note that

$$f=\frac{x}{4}Df+\left(\frac{3x}{4}+1\right)$$

Assume f is inseparable and they share a solution α. Put $x=\alpha$ above to get

$$\left(\frac{3}{4}\alpha+1\right)=f(\alpha)-\frac{\alpha}{4}Df(\alpha)=0\Rightarrow\alpha=-\frac{4}{3}$$

It is easy to check $f\left(-\frac{4}{3}\right)\neq 0$ which contradicts the fact that α is a solution. Therefore, no such α exists and f is separable.

Problem 3.2

Show that any field of characteristic 0 is perfect.

Solution: Let F be a characteristic 0 field and let $f=\sum_{i=0}^{n}c_ix^i$ be irreducible. Let α be a root of the polynomial. Then f is the minimal polynomial of α over F. We claim that multiplicity of α in f is 1. If f has degree 1, then it has a single root α and we are done. Otherwise, we have $Df(\alpha)=0$. Now, if we assume f has degree n then $Df=\sum_{i=0}^{n-1}(i+1)c_{i+1}x^i$. As $c_n\neq 0$, and $char(F)=0$, $nc_n\neq 0$. Therefore, $Df\neq 0$. But as $Df(\alpha)=0$ and $deg(Df)=deg(f)-1$, p cannot be the minimal polynomial, which is a contradiction. Therefore, $Df(\alpha)\neq 0$ and multiplicity of α in f is 1. So F is perfect.

Problem 3.3

Let F be a field of characteristic p. Show that the map $\phi : F\to F$ defined by $\phi(a)=a^p$ is a homomorphism.

Solution: We know for any prime p(characteristic of a field is always prime) and $1<k<p$, $\binom{p}{k}$ is divisible by p. For $a,b\in F$

$$\phi(a)+\phi(b)=a^p+b^p=a^p-1+\sum_{i=1}^{p-1}\binom{p}{i}(a)^i(b)^{p-i}=(a+b)^p=\phi(a+b)$$

As

1. $\phi(a+b)=\phi(a)+\phi(b)$
2. $\phi(ab)=(ab)^p=a^pb^p=\phi(a)\phi(b)$

ϕ is a homomorphism.

Problem 3.4

Show that any algebraic extension of a perfect field is perfect.

Solution:

Problem 3.5

A nonzero polynomial $f(x) \in F[x]$ is separable if and only if it is relatively prime to its derivative in $F[x]$ (i.e., $(f(x), f'(x)) = 1$).

Solution:

f is separable $\Rightarrow (f, f') = 1$

Assume to the contrary that $(f, f') = p \neq 1$. Then all roots of p is a common root of both f and f'. Therefore, f is not separable which is a contradiction.

$(f, f') = 1 \Rightarrow f$ is separable

Assume f and f' are inseparable. Then there exists α such that $f(\alpha) = f'(\alpha) = 0$. Let p be the minimal polynomial of α. Then $p \mid f, p \mid f'$ and so $p \mid (f, f')$. But this is a contradiction as 1 is a scalar and non-scalar polynomial can divide it.

Problem 3.6

Is $f(X) = X^6 + X^5 + X^4 + 2X^3 + 2X^2 + X + 2 \in \mathbb{F}_3[X]$ a separable polynomial?

Solution: In $\mathbb{F}_3$, $f' = 2x^4 + +x^3 + x$. We use Euclid's algorithm to compute the GCD.

$$x^6 + x^5 + x^4 + 2x^3 + 2x^2 + x + 2 = (2x^2 + x)(2x^4 + x^3 + x) + (x^2 + x + 2)$$

$$2x^4 + x^3 + x = (x^2 + x + 2)(2x^2 + 2x) + x$$

$$x^2 + x + 2 = x(x + 1) + 2$$

Therefore, $(f, f') = 1$ and by problem 3.5, f is separable.

4 Problem Sheet 4

Problem 4.1

Let F be a finite field with p^n elements. Show that the map $\phi : F \to F$ defined by $\phi(a) = a^p$ is an isomorphism. Show that ϕ has order n.

Solution: As F is finite the characteristic of F is a prime. Let it be k. Then for $a \in K$, $ka = 0$. As $(F, +)$ forms a group, by Lagrange's theorem, $k|p^n$. The only prime which divides p^n is p, so $k = p$. By problem 3.3, ϕ is a group homomorphism. Let $\phi(\alpha) = 0$. Then $\alpha^p = 0 \Rightarrow \alpha = 0$. Therefore, $\ker(\phi) = \{0\}$ and ϕ is one-one. As F is finite, any injective map from F to itself is a bijection. Therefore, ϕ is an isomorphism.

Problem 4.2

Show that if m divides n, $x^{p^m} - x$ divides $x^{p^n} - x$

Solution:

Lemma 6. *If $m|n$ then $x^m - 1|x^n - 1$.*

Proof. Write $n = mk$. Then
$$x^n - 1 = x^{mk} - 1 = (x^m - 1)\left(\sum_{i=0}^{k-1} x^m\right)$$
□

Now as $m|n$,
$$p^m - 1|p^n - 1 \Rightarrow x^{p^m-1} - 1|x^{p^n-1} - 1 \Rightarrow x(x^{p^m-1} - 1)|x(x^{p^n-1} - 1) \Rightarrow x^{p^m} - x|x^{p^n} - x$$

Problem 4.3

Investigate whether there is a finite field with the following number of elements and construct such a field if it exists.
(1) 72.
(2) 625.

Solution:

1. No. Finite fields always have p^n elements where p is a prime. 72 is not of this form.
2. Yes. $625 = 5^4$. As 5 is a prime, such a field exists. It is the splitting field of $x^{625} - x$ over $\mathbb{F}_5$

Problem 4.4

Let F be a field with $ch(F) = p$. Give an example to show that the map $\phi : F \to F$ defined by $\phi(a) = a^p$ need not be an automorphism of F if F is an infinite field.

Solution: Let $p = 3$ and $F = \mathbb{F}_3[x]$. If ϕ is an automorphism, then there exists $f \in \mathbb{F}_3[x]$ such that $\phi(f) = f^3 = x^3 + x$ and $deg(f^3) = 3deg(f) = 3 \Rightarrow deg(f) = 1$. Let $f = x - a$. Then $f^3 = x^3 - a^3$, which cannot be equal to $x^3 + x$. Therefore, no such f exists and ϕ is not an automorphism.

Problem 4.5

Let $K|F$ be a finite extension where F is a finite field. Show that $|K| = (|F|)^n$ for some $n \in \mathbb{N}$.

Solution: As F, K are finite fields, $|K| = p^\alpha$ for some primes p. As F is a subfield, characteristic of F is also p and $|F| = p^\beta$ where $\beta < \alpha$. We know $\beta|\alpha$ and therefore there exists c such that $\beta c = \alpha \Rightarrow (p^\beta)^c = p^\alpha \Rightarrow |F|^c = |K|$

Problem 4.6

If $f(x) \in F[x]$ is separable then the splitting field of $f(x)$ over F is separable over F.

Solution:

Problem 4.7

Show that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ is simple by showing $\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$

Solution: Note that $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) \hookrightarrow \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. By following the steps similar to problem 1.1, we get $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = 6$. Let p be the minimal polynomial of $\sqrt{2} + \sqrt[3]{3}$ over $\mathbb{Q}$. p is not linear. We show p is not quadratic or cubic. Assume p is quadratic. Then $p = x^2 + bx + c$ for some $b, c \in \mathbb{Q}$. Therefore:
$$(\sqrt{2} + \sqrt[3]{3})^2 + b(\sqrt{2} + \sqrt[3]{3}) + c = 0$$
$$\Rightarrow \sqrt{2} = \frac{-c - b\sqrt[3]{3} - \sqrt[3]{3}^2 - 2}{b + 2\sqrt[3]{3}} \in \mathbb{Q}(\sqrt[3]{3})$$

Which is not true. A similar argument shows p is not cubic. Therefore $deg(p) > 3$ and by tower lemma, $deg(p) = [\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) : \mathbb{Q}]|6$. Therefore $[\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) : \mathbb{Q}] = 6$ and $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}]|[\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) : \mathbb{Q}] = 1 \Rightarrow [\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}]$

Problem 4.8

Prove that every element of a finite field can be written as a sum of two squares.

Solution:

Lemma 7. *For $a \in F, a \neq 0$, if a has a square root, then a has exactly 2 square roots.*

Proof. Let $x^2 = a$ and let $(x + y)^2 = a$. Then it follows that $2xy + y^2 = 0 \Rightarrow y(2x + y) = 0$. Therefore, $y = 0$ or $y = -2x$. Therefore, there are exactly two roots: $x, -x$. For $a = 0, x = -x = 0$ $\square$

It follows that $S = \{a | \exists\ x \text{ such that } x^2 = a\}$ has exactly $\frac{|F|-1}{2} + 1 = \frac{|F|+1}{2}$ elements. For any $a \in F$ consider $S_a = \{a - s | s \in S\}$. Then S_a also has $\frac{|F|+1}{2}$ elements. As $|S| + |S_a| = |F| + 1 > |F|$ by pigeonhole principle, $S \cap S_a \neq \phi$. Let e be an element in the intersection. Then $e = n^2 = a - m^2$ for $n, m \in F$. Therefore, $a = n^2 + m^2$.