Galois theory - Problem Set 1

To be solved on Thursday 25.01

Chapter 11.1

Problem 1. Let R be an integral domain.

(a) Let $a, x, y \in R$, $a \neq 0$. Show that if $ax = ay$, then $x = y$.

(b) Let $a, b \in R$. Show that if $a \mid b$ and $b \mid a$, then there exists a unit $u \in R$ such that $b = ua$.

(c) Let $a, u \in R$ where u is a unit. Show that a is a unit if and only if ua is a unit.

(d) Let $a, b, u \in R$ where u is a unit. Show that $a \mid b$ if and only if $ua \mid b$.

(e) Let $p \in R$. Show that if p is prime, then p is irreducible.

(f) Let $p, u \in R$ where u is a unit. Show that p is irreducible respectively prime if and only if pu is irreducible respectively prime.

(g) Let $a, p \in R$ with a not a unit and p prime. Show that if $a \mid p$, then there exists a unit $u \in R$ such that $a = up$.

(h) Let $a, b \in R$. Show that $a \mid b$ if and only if $(b) \subseteq (a)$.

Problem 2. Let R be an integral domain such that for every $x, y \in R$ we have that $\gcd(x, y)$ exists. Let $a, b, c \in R$.

(a) (Exercise 11.1.1 in the book.) Show that $\gcd(ca, cb) = c \gcd(a, b)$.

(b) (Exercise 11.1.2 in the book.) Show that if $\gcd(a, b) = 1$ and if $a \mid c$ and $b \mid c$, then $ab \mid c$.

(c) (Exercise 11.1.3 in the book.) Show that if $\gcd(a, b) = 1$ and $b \mid ac$, then $b \mid c$.

Problem 3. (Exercise 11.1.8 in the book.) Show that in the ring $\mathbb{Z}[\sqrt{-3}]$ the gcd of 4 and $2 + 2\sqrt{-3}$ does not exist.

Chapter 11.3

Problem 4. Let $k \in \mathbb{Z}$ and consider the map $\phi : \mathbb{Z}[\sqrt{k}] \to \mathbb{Z}$ defined by $\phi(a + b\sqrt{k}) = |a^2 - kb^2|$.

(a) Show that ϕ is multiplicative, that is for all $a, b, c, d \in \mathbb{Z}$ we have $\phi((a + b\sqrt{k})(c + d\sqrt{k})) = \phi(a + b\sqrt{k})\phi(c + d\sqrt{k})$.

(b) Show that for all $a, b, c, d \in \mathbb{Z}$ we have that if $(a + b\sqrt{k}) \mid (c + d\sqrt{k})$, then $\phi(a + b\sqrt{k}) \mid \phi(c + d\sqrt{k})$.

(c) Show that $a + b\sqrt{k} \in \mathbb{Z}[\sqrt{k}]$ is a unit if and only if $\phi(a + b\sqrt{k}) = 1$.

Problem 5. (Exercise 11.3.4 in the book.) Let $a = 3 + 2i$ and $b = 2 - 3i$ be two elements in $\mathbb{Z}[i]$. Find q and r in $\mathbb{Z}[i]$ such that $a = bq + r$ and $\phi(r) < \phi(b)$, where $\phi(x + yi) = x^2 + y^2$.

Problem 6. (Exercise 11.3.2 in the book) Show that the ring $\mathbb{Z}[\sqrt{2}]$ is a euclidean domain and a UFD. Explain why in the UFD $\mathbb{Z}[\sqrt{2}]$ we have

$$(5+\sqrt{2})(2-\sqrt{2}) = (11-7\sqrt{2})(2+\sqrt{2})$$

even though each of the factors is irreducible.

Problem 7. (Exercise 11.3.8 in the book.) Show that $\mathbb{Z}[\sqrt{-6}]$ is not a euclidean domain.

Chapter 15.1

Problem 8. (Exercise 15.1.1 in the book.) Show that $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_7[x]$ is irreducible over the field $\mathbb{Z}_7$.

Problem 9. (Exercise 15.1.4 in the book.) Show that $f(x) = x^3 + ax^2 + bx + 1 \in \mathbb{Z}[x]$ is reducible over $\mathbb{Z}$ if and only if either $a = b$ or $a + b = -2$.

Problem 10. (Exercise 15.1.2 in the book.) Show that $f(x) = x^4 + 8 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

Problem 11. Prove or disprove that $\sqrt[19]{17000}$ is a rational number.

Problem 12. Find the unique factorization of $f(x) = x^4 + x^3 - 3x^2 + 3x + 3 \in \mathbb{Z}_5[x]$

Chapter 15.2

Problem 13. (Exercise 15.2.4 in the book.) Find the smallest extension of $\mathbb{Q}$ having a root of $f(x) = x^2 + 4 \in \mathbb{Q}[x]$.

Problem 14. (Exercise 15.2.1 in the book.) Show that $p(x) = x^2 - x - 1 \in \mathbb{Z}_3[x]$ is irreducible over $\mathbb{Z}_3$. Show that there exists an extension K of $\mathbb{Z}_3$ with nine elements having all roots of $p(x)$.

Problem 15. (Exercise 15.2.2 in the book.) Show that $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$. Find (if it exists) an extension K of $\mathbb{Q}$ having all roots of $x^3 - 2$ such that $[K : \mathbb{Q}] = 6$.

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 16. (Chapter 11.1) Give an example of an integral domain R and an element $r \in R$ such that $r \neq 0$, r is not a unit, r is not irreducible, and r is not a product of irreducible elements. (*Hint*: use a suitable subring of $\mathbb{Q}[x]$.)

Problem 17. (Chapter 15.1) Let $n \geq 1$ and $f(x) = (x-1)(x-2)\cdot\ldots\cdot(x-n)+1$.

(a) For a general polynomial $p(x) \in \mathbb{Z}[x]$, show that for any two integers $m, l \in \mathbb{Z}$, the integer $m-l$ divides $p(m) - p(l)$.

(b) Show that $f(x)$ is irreducible over $\mathbb{Z}$ if and only if $n \neq 4$.