# GRV II final with answers.

1. Let $R$ be an integral domain and let $r \in R$ be not zero and not a unit.

   (a) Give definition of: $p$ is prime.

   $p|ab \implies p|a$ or $p|b$

   (b) Give definition of: $p$ is irreducible.

   $p = ab \implies a$ is a unit or $b$ is a unit (which implies that the other is an associate of $p$).

   (c) Which one (prime or irreducible) implies the other one?

   Prime $\implies$ irreducible. If $p = ab$ and $p$ is prime then $p|a$ or $p|b$. Assume $p|a$ (the case $p|b$ is the same). Then $a = pr$ for some $r$. Then $p \cdot 1 = ab = p \cdot rb$ but then $rb = 1$ (the cancellation law holds in an integral domain) so then $b$ is a unit.

2. Let $f \in \mathbb{Q}[x]$ be monic and not constant. Suppose that $e^2 = e$ has only two solutions in the ring $\mathbb{Q}[x]/(f)$. Show that $f = g^d$ for some $d \geq 1$ and some irreducible $g \in \mathbb{Q}[x]$.

   If $f$ is not of this form then we can factor $f = gh$ with $g, h$ not constant and coprime. Then $\mathbb{Q}[x]/(f) \cong \mathbb{Q}[x]/(g) \times \mathbb{Q}[x]/(h)$ by the Chinese Remainder Theorem, and in that latter ring the equation $e^2 = e$ has $> 2$ solutions: $(0,0), (0,1), (1,0)$, and $(1,1)$.

3. Let $p$ be a prime number.

   (a) Up to isomorphism, how many $\mathbb{Z}$-modules exist with precisely $p^4$ elements? List all.

   There are ***five*** partitions of 4, namely: $4$, $1+3$, $2+2$, $1+1+2$, and $1+1+1+1$ which correspond to: $\mathbb{Z}/(p^4)$, $\mathbb{Z}/(p) \times \mathbb{Z}/(p^3)$, $\mathbb{Z}/(p^2) \times \mathbb{Z}/(p^2)$, $\mathbb{Z}/(p) \times \mathbb{Z}/(p) \times \mathbb{Z}/(p^2)$, and $\mathbb{Z}/(p) \times \mathbb{Z}/(p) \times \mathbb{Z}/(p) \times \mathbb{Z}/(p)$.

   (b) Up to isomorphism, how many $\mathbb{F}_p[x]$-modules exist with precisely $p^4$ elements?

   Let $R = \mathbb{F}_p[x]$ then by the classification of modules over a PID we find that these modules are of the form $R/(a_1) \oplus \cdots \oplus R/(a_k)$ with $a_i$ monic, $a_1|a_2|\cdots$ and the degrees of the $a_i$ being a partition of 4.
   Partitions:
   $4 = 4$: $p^4$ choices ($a_1$ is an arbitrary monic degree 4 polynomial)
   $4 =$ 1+3: $p^3$ choices ($p$ for $a_1$ and $p^2$ for $a_2 = \text{deg2} \cdot a_1$)
   $4 =$ 2+2: $p^2$ choices ($a_1 = a_2$ is an arbitrary monic deg2 poly)
   $4 =$ 1+1+2: $p^2$ choices ($p$ for $a_1 = a_2$, and $p$ for $a_3 = \text{deg1} \cdot a_1$)
   $4 =$ 1+1+1+1: $p$ choices for $a_1 = a_2 = a_3 = a_4$.
   Total: $p^4 + p^3 + 2 \cdot p^2 + p$ choices.

4. Let $K$ be the splitting field of $x^6 - 2$ over $\mathbb{Q}$.

   (a) What is $[K : \mathbb{Q}]$? Explain.

The field $F := \mathbb{Q}(\sqrt[6]{2})$ has degree 6 over $\mathbb{Q}$ because $x^6-2$ is irreducible (Eisenstein) over $\mathbb{Q}$. The splitting field of $x^6 - 2$ also contains $\zeta_6$, which has degree $\phi(6) = 2$ over $\mathbb{Q}$. Then $\zeta_6$ also has degree 2 over $F$ because $\zeta_6 \notin \mathbb{R} \supset F$. So the splitting field $K = F(\zeta_6) = \mathbb{Q}(\sqrt[6]{2}, \zeta_6)$ has degree $6 \cdot 2 = 12$ over $\mathbb{Q}$.

(b) How many subfields $E$ does $K$ have with $[E : \mathbb{Q}] = 4$?

If $[E : \mathbb{Q}] = 4$ then $[K : E] = 12/4 = 3$.
The 6 complex roots of $x^6 - 2$ are vertices of a regular hexagon, and the Galois group $G =< \sigma, \tau >$ acts on these 6 roots as $D_{2\cdot 6}$, where $\tau$ = complex conjugation (acts as a reflection, fixed field is $F$) and where $\sigma$ sends $\zeta_6$ to itself and sends $\sqrt[6]{2}$ to $\zeta_6 \sqrt[6]{2}$ (this acts as a rotation of order 6).

The dihedral group $D_{2\cdot n}$ contains $n$ rotations (whose orders are divisors of $n$) and $n$ reflections (those have order 2). The group $D_{2\cdot 6}$ has only 2 elements of order 3, namely namely $\sigma^2$ and $\sigma^4$. So there is only subgroup of order 3, namely $< \sigma^2 >$ and hence there is only **one** subfield $E$ with $[K : E] = 3$.

(Note: $< \sigma^2 >$ is a normal subgroup so $E$ should be Galois over $\mathbb{Q}$. Indeed: $E = \mathbb{Q}(\sqrt{2}, \zeta_6) = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$.)

5. Let $p$ be a **prime number** $> 2$ and let $K = \mathbb{Q}(\zeta_p)$.

(a) Show that $K$ has precisely one subfield $F$ with $[K : F] = 2$.

$K$ is Galois over $\mathbb{Q}$ with group $G = (\mathbb{Z}/(p))^* \cong C_{p-1}$. A cyclic group $G$ with even order has precisely one subgroup $< \tau >$ of order 2
($F$ is the fixed field of $< \tau >$).

(b) Show that $K$ has precisely one subfield $E$ with $[E : \mathbb{Q}] = 2$.

A cyclic group $G$ with even order $p - 1$ has precisely one subgroup $H$ of order $(p - 1)/2$ ($E$ is the fixed field of $H$).

(c) Show that $E \subset \mathbb{R}$ if and only if $p \equiv 1 \bmod 4$.

$E \subseteq \mathbb{R}$ if and only if $E$ is fixed under $\tau$ (= complex conjugation). $E = K^H$ is fixed under $\tau$ if and only if $\tau \in H$. But $H$ is cyclic of order $(p - 1)/2$ so it contains $\tau$ if and only if $(p - 1)/2$ is even.

6. Let $K/\mathbb{Q}$ be Galois with group $G$ and let $b \in K$ with $b \neq 0$. Show that there exists $\sigma \in G$ with $\sigma(b) = -b$ if and only if $b \notin \mathbb{Q}(b^2)$.

Let $E_1 = \mathbb{Q}(b)$ and $E_2 = \mathbb{Q}(b^2)$. Since $K$ is Galois over $\mathbb{Q}$, it follows that $E_1, E_2$ are fixed fields of some groups $H_1, H_2$ of $G$. Now $H_1 \subseteq H_2$ because $E_2 \subseteq E_1$, and both $\subseteq$ are an equality if and only if $b \in E_2$.

If $\sigma$ sends $b$ to $-b$ and $b \neq 0$ then $\sigma \notin H_1$ but $\sigma(b^2) = (-b)^2 = b^2$ so $\sigma \in H_2$. Then $H_1 \neq H_2$ so $b \notin E_2$.

Conversely, if $b \notin E_2$ then $E_1 \neq E_2$ so $H_1 \subsetneq H_2$ so there exists $\sigma \in H_2$ with $\sigma \notin H_1$. That means $\sigma(b^2) = b^2$ and $\sigma(b) \neq b$, which must then differ by a minus sign since their squares are the same.