Solutions to Final exam **Math 5590H**

50% **1.** *Let $D \neq 0, 1$ be a square-free integer, and let $R = \mathbb{Z}[\omega]$ where $\omega = \sqrt{D}$ or $\omega = \frac{1+\sqrt{D}}{2}$ if $D = 1 \bmod 4$. Let $p \in \mathbb{N}$ be a prime.*

(**a**) *Prove that $R \cong \mathbb{Z}[x]/(f)$, where $f = x^2 - D$ if $\omega = \sqrt{D}$ and $f = x^2 - x + \frac{1-D}{4}$ if $\omega = \frac{1+\sqrt{D}}{2}$.*

Solution. Let $\varphi\colon \mathbb{Z}[x] \longrightarrow \mathbb{C}$ be the evaluation homomorphism at ω, $\varphi(g) = g(\omega)$, $g \in \mathbb{Z}[x]$. The range of φ is $\mathbb{Z}[\omega] = R$, the kernel is the ideal $I = \{g \in \mathbb{Z}[x] : g(\omega) = 0\}$, so that $R \cong \mathbb{Z}[x]/I$. We have $f \in I$ (in the case $\omega = \frac{1+\sqrt{D}}{2}$, $\omega^2 = \frac{1+D}{4} + \frac{\sqrt{D}}{2} = \frac{-1+D}{4} + \frac{1+\sqrt{D}}{2} = \omega - \frac{1-D}{4}$), and we need to show that $I = (f)$. Assume not; $\mathbb{Z}[x]$ is a PID, so $I = (g)$ for some $g \in \mathbb{Z}[x]$, and then $g \,\big|\, f$. f is monic and of degree 2, so, if g is not an associate of f, we must have $\deg g = 1$ and (since the senior coefficient of g must be ± 1) we may assume that g is monic. However, $\omega \notin \mathbb{Z}$, so is not a root of a linear monic polynomial $g \in \mathbb{Z}[x]$.

(**b**) *Prove that $R/(p) \cong \mathbb{F}_p[x]/(f)$ (where $\mathbb{F}_p = \mathbb{Z}_p$).*

Solution.

$$R/(p) \cong (\mathbb{Z}[x]/(f))/(p) \cong \mathbb{Z}[x]/(f, p) \cong (\mathbb{Z}[x]/(p)[x])/(f) \cong \mathbb{F}_p[x]/(f).$$

(By (p) I denote the ideal generated by p in R; the ideal generated by p in $R[x]$ is then $(p)[x]$.)

(**c**) *Prove that, under the isomorphism in (b), the conjugation automorphism of R acts on $\mathbb{F}_p[x]/(f)$ by $x \mapsto -x$ if $\omega = \sqrt{D}$ and $x \mapsto 1 - x$ if $\omega = \frac{1+\sqrt{D}}{2}$.*

Solution. The conjugation automorphism acts on R by $\sqrt{D} \mapsto -\sqrt{D}$; so, if $\omega = \sqrt{D}$, then $\omega \mapsto -\omega$, and if $\omega = \frac{1+\sqrt{D}}{2}$, then $\omega \mapsto \frac{1-\sqrt{D}}{2} = 1 - \omega$. Under isomorphism in (b), $\omega \leftrightarrow x$, so conjugation maps $x \mapsto -x$ if $\omega = \sqrt{D}$ and $x \mapsto 1 - x$ if $\omega = \frac{1+\sqrt{D}}{2}$.

(**d**) *Prove that*

(i) *if f has no roots in $\mathbb{F}_p$, p is inert (is prime) in R;*

(ii) *if f has two distinct roots in $\mathbb{F}_p$, then p splits in R into a product of two distinct maximal ideals: $(p) = P_1 P_2$;*

(iii) *and if f has a double root (a root of multiplicity two) in $\mathbb{F}_p$, then p ramifies in R: $(p) = P^2$, where P is a maximal ideal in R.*

Solution. The ring $\mathbb{F}_p[x]$ is a PID.

(i) If the polynomial f is irreducible in this ring, then $R/(p) \cong \mathbb{F}_p[x]/(f)$ is a field, so p is prime, that is, p is inert.

(ii) If f splits in $\mathbb{F}_p[x]$ into distinct factors, $f = (x - \alpha)(x - \beta)$ with $\alpha \neq \beta$, then $R/(p) \cong \mathbb{F}_p[x]/(f)$ has non-associate zero divisors $x - \alpha$ and $x - \beta$, that is, p splits. Let P_1 and P_2 be the preimages in $R \cong \mathbb{Z}[x]/(f)$ of the maximal ideals $(x-\alpha)$ and $(x-\beta)$ in $\mathbb{F}_p[x]/(f)$, then P_1 and P_2 are maximal ideals in R with $(p) = P_1 P_2 = P_1 \cap P_2$.

(iii) If f is a square, $f = (x-\alpha)^2$, in $\mathbb{F}_p[x]$, then $R/(p) \cong \mathbb{F}_p[x]$ has a nontrival nilradical, that is, p ramifies. We then have $(p) = P^2$ in R, where P is the preimage in $R \cong \mathbb{Z}[x]/(f)$ of the maximal ideal $(x - \alpha)$ in $\mathbb{F}_p[x]/(f)$.

(**e**) *If p splits in R, $(p) = P_1 P_2$, prove that P_1 and P_2 are conjugate, $P_2 = \overline{P}_1$; if p ramifies, $(p) = P^2$, then P is self-conjugate, $\overline{P} = P$.*

Solution. If p splits, $(p) = P_1 P_2$, then the conjugation in R preserves the ideal (p) and so either preserves both P_1 and P_2 or swithes them. P_1 and P_2 are the preimages in $R \cong \mathbb{Z}[x]/(f)$ of the ideals $(x - \alpha)$ and $(x - \beta)$ in $\mathbb{F}_p[x]/(f)$. If $\omega = \sqrt{D}$, $\beta = -\alpha$; if $\omega = \frac{1+\sqrt{D}}{2}$, $f = x^2 - x + \frac{1-D}{4}$, so $\alpha + \beta = 1$, so $\beta = 1 - \alpha$. The conjugation sends $x \mapsto -x$ or $1 - x$, so sends $(x - \alpha) \mapsto (-x - \alpha) = (x + \alpha) = (x - \beta)$ or $(x - 1 + \alpha) = (x - \beta)$; hence, it sends P_1 to P_2 (and P_2 to P_1).

If p ramifies, $(p) = P^2$, the ideal P is the radical of (p), so is preserved by conjugation.

(**f**) *In the case $\omega = \sqrt{D}$, prove that p ramifies if and only if $p = 2$ or $p \,\big|\, D$.*

Solution. If $f = x^2 - D$ and p ramifies, then $x^2 - D = (x - \alpha)^2 = x^2 - 2\alpha + \alpha^2$, so $2\alpha = 0$ and $\alpha^2 = D$ in $\mathbb{F}_p$. This is so iff $2 = 0$, or $\alpha = 0$ and then $D = \alpha^2 = 0$ in $\mathbb{F}_p$. In the first case $p = 2$, in the second $p \,\big|\, D$.

Conversely, if $p = 2$ then $x^2 - D = x^2 + 1 = (x + 1)^2$ or $x^2 - D = x^2$ in $\mathbb{F}_2[x]$; if $p \,\big|\, D$ then $x^2 - D = x^2$ in $\mathbb{F}_p[x]$.

(**g**) *Prove that* 7 *is irreducible but not prime in* $\mathbb{Z}[\sqrt{-5}]$*, and that* 11 *is prime in* $\mathbb{Z}[\sqrt{-5}]$.

Solution. Let $D=-5$, $R=\mathbb{Z}[\sqrt{-5}]$, $f=x^2+5$.

7 is irreducible in R and if $\alpha=a+b\sqrt{-5}\in R$ with $a,b\in\mathbb{Z}$ divides 7, then $N(\alpha)=a^2+5b^2$ divides $N(7)=49$; but if $N(\alpha)=1$ then α is a unit, if $N(\alpha)=49$ then $7/\alpha$ is a unit, and $N(\alpha)=a^2+5b^2=7$ is impossible.

f is reducible in $\mathbb{Z}_7[x]$, $f=(x-3)(x-4)$, so 7 splits (is not prime) in R. (And indeed, $7\,|\,14=(3+\sqrt{-5})(3-\sqrt{-5})$ whereas $7\nmid 3\pm\sqrt{-5}$. The prime factorization in R of the ideal (7) is $(7)=(7,3+\sqrt{-5})(7,3-\sqrt{-5})$.)

In $\mathbb{Z}_{11}$ f has no roots ($1^2=10^2=1$, $2^2=9^2=4$, $3^3=8^2=9$, $4^2=7^2=5$, $5^2=6^2=4$, all $\neq -5=6$), so f is irreducuble in $\mathbb{Z}_{11}[x]$, and 11 is inert (is prime) in R.

10% **2.** *Prove that the quotient ring* $\mathbb{Z}[x]/(2x-1)$ *is isomorphic to the ring of fractions* $D^{-1}\mathbb{Z}$ *where* $D=\{2^n,\ n\in\mathbb{N}\}$.

Solution. Consider the (evaluation) homomorphism $\varphi\colon\mathbb{Z}[x]\longrightarrow\mathbb{Q}$ defined by $\varphi(g)=g(1/2)$. The range of φ is $\mathbb{Z}[1/2]=D^{-1}\mathbb{Z}$. The kernel of φ is the ideal $(2x-1)$: indeed, $\varphi(2x-1)=0$, and if $g(1/2)=0$ for $g\in\mathbb{Z}[x]$, then g is divisible by $x-1/2$ in $\mathbb{Q}[x]$, so is divisible by $2x-1$ in $\mathbb{Z}[x]$ by Gauss's lemma since $2x-1$ is primitive. Hence, $\mathbb{Z}[x]/(2x-1)\cong D^{-1}\mathbb{Z}$.

3. *Let* R *be a PID.*

15% (**a**) *Prove that every prime ideal in* $R[x]$ *can be generated by at most two generators.*

(Notice that the assertion doesn't hold true for non-prime ideals: in $\mathbb{Z}[x]$ the ideal $(4,2x,x^2)$ cannot be generated by two elements.)

Solution. Let P be a nonzero prime ideal in $R[x]$.

Case 1: $P\cap R\neq 0$. Then $P\cap R$ is a prime ideal in R, so $P\cap R=(p)$ for some prime $p\in R$. Then $K=R/(p)$ is a field, and we have a surjective homomorphism $\varphi\colon R[x]\longrightarrow K[x]$. $\varphi(P)$ is an ideal in the PID $K[x]$, so $\varphi(P)=(\varphi(f))$ for some $f\in R[x]$. I claim that $P=(p,f)$. Indeed, for any $g\in P$, $\varphi(g)=\varphi(h)\varphi(f)=\varphi(hf)$ for some $h\in R[x]$, so $g-hf\in\ker\varphi$, so $g-hf\in(p)[x]$, so $g-hf=pr$, $g=hf+pr$ for some $r\in R[x]$.

Case 2: $P\cap R=0$. Let F be the field of fractions of R, $F=D^{-1}R$ where $D=R\setminus\{0\}$; I will see R as a subring of F. Since $P\cap D=\emptyset$, the set $\widetilde{P}=D^{-1}P$ is a proper ideal (namely, (P)) in $F[x]$. $F[x]$ is a PID, so there is a nonconstant $f\in F[x]$ such that $\widetilde{P}=(f)$; after multiplying f by an element of F we may assume that $f\in R[x]$ and is primitive. I claim that $P=(f)$. Indeed, for every $g\in P$ we have $g\in\widetilde{P}$, so $g=cf$ where $c\in F$ is the content of g and so, $c\in R$. So, $P\subseteq(f)$. On the other hand, let $g=cf$ with nonzero $c\in R$ being any element of P; since P is prime, we have $c\in P$ or $f\in P$; since $P\cap R=0$, $c\neq 0$, so $f\in P$, so $(f)\subseteq P$.

5% (**b**) *If* S *is a ring containing* R *and generated by a single element over* R, $S=R[\alpha]$*, prove that every prime ideal in* S *can be generated by at most two elements.*

Solution. S is the image of $R[x]$ under the evaluation homomorphism $g\mapsto g(\alpha)$, and every prime ideal in S is the image of a prime ideal in $R[x]$, so can be generated by at most two elements.

10% **4.** *Prove that the polynmial* $6x^5-55x^3+50x^2+15$ *is irreducible over the field* $\mathbb{Q}[i]$ *(that is, in the ring* $\mathbb{Q}[i][x]$*).*

Solution. $\mathbb{Q}[i]$ is the field of fractions of the UFD $\mathbb{Z}[i]$, so any polynomial from $\mathbb{Z}[i][x]$ is irreducible in this ring iff it is irreducible in $\mathbb{Q}[i][x]$. And the polynomial under question is irreducible in $\mathbb{Z}[i][x]$ by the Eisenstein criterion with respect to the prime element $\alpha=2+i$ of $\mathbb{Z}[i]$; $\alpha\nmid 6$ (the prime factorization of 6 in $\mathbb{Z}[i]$ is $6=(1+i)(1-i)3$); $\alpha\,|\,5$ and 5 divides all other coefficients of the polynomial; and $\alpha^2\nmid 15$ (since the prime factorization of 15 is $15=3(2+i)(2-i)$).

10% **5.** *A group* N *is said to be complete if the center of* N *is trivial and every automorphism of* N *is inner. Show that if* G *is a group,* $N\trianglelefteq G$*, and* N *is complete, then* $G=N\times C_G(N)$.

Solution. We have $N \cap C_G(N) = Z(N)$, the center of N, so $N \cap C_G(N) = 1$ by assumption. For every $c \in N$ and $d \in C_G(N)$, c and d commute by the definition of $C_G(N)$. It remains to show that $G = NC_G(N)$. Let $a \in G$. Let φ be the inner automorphism of G defined by conjugation by a, $\varphi(b) = aba^{-1}$, $b \in G$. Since $N \trianglelefteq G$, $\varphi(N) = N$, so $\varphi|_N$ is an automorphism of N. By assumption, there is $c \in N$ such that $\varphi(b) = cbc^{-1}$ for all $b \in N$, that is, $aba^{-1} = cbc^{-1}$ for all $b \in N$. Put $d = c^{-1}a$; then $dbd^{-1} = c^{-1}aba^{-1}c = c^{-1}cbc^{-1}c = b$ for all $b \in N$. Hence, $d \in C_G(N)$, so $a = cd$ for $c \in N$ and $d \in C_G(N)$.

15% **6.** *Prove that no group of order* $2004 = 2^2 \cdot 3 \cdot 167$ *is simple. Give an example of a group of order* 2004 *in which a Sylow* 3*-subgroup is not normal.*
(This problem was given to you by mistake, it was too easy, sorry.)

Solution. Let G be a group of order 2004. The Sylow number n_{167} of G is equal to 1 modulo 167 and divides $2^2 \cdot 3 = 12$, so $n_{167} = 1$, so the Sylow 167-subgroup of G is unique and normal, so G is not simple.

As an example of such G with non-normal Sylow 3-subgroups we can take $G = A_4 \times \mathbb{Z}_{167}$: the group A_4 has order 12 and contains four Sylow 3-subgroups, hence G also has four Sylow 3-subgroups.